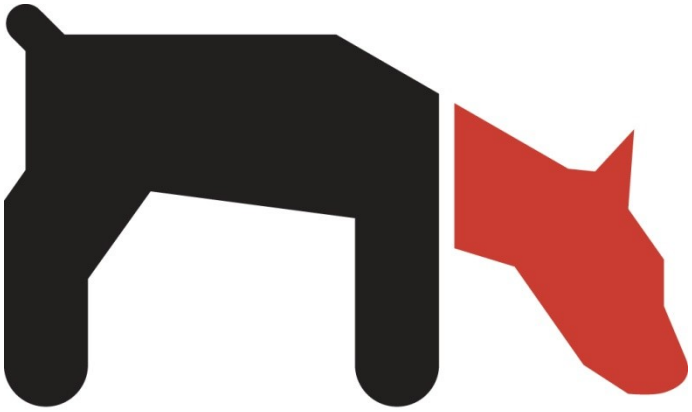


REDDOXX

User Manual

Version 2029

- **User Console**
- **Outlook AddIn**
- **Web Interface**

www.reddoxx.com

Copyright

©2011 by REDDOXX GmbH

REDDOXX GmbH
Neue Weilheimer Str. 14

D-73230 Kirchheim

Fon: +49 (0)7021 92846-0
Fax: +49 (0)7021 92846-99

Email: info@reddoxx.com
Internet: http://www.reddoxx.com
Support: http://support.reddoxx.net

Revision number: 3.5

Last alteration: 24.07.2012

This manual was prepared with great care. However, REDDOXX GmbH and the author cannot assume any legal or other liability for possible errors and their consequences.

No responsibility is taken for the details contained in this manual. Subject to alteration without notice. REDDOXX GmbH does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement.

This manual is protected by copyright law. REDDOXX GmbH reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of REDDOXX GmbH. The latter especially applies for data processing systems.

REDDOXX GmbH also reserves all communication rights (lectures, radio and television).

The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of REDDOXX GmbH.

This issue replaces all earlier ones and orients itself on the appliance with respect to naming.

Table of Contents

1 Introduction and Start 4
1.1 REDDOXX User Console (User GUI) 4
1.2 REDDOXX Outlook AddIn 4
1.3 REDDOXX Web Interface 4
2 Login 5
2.1 Login with the User Console 5
2.2 Login with MS Outlook 5
2.3 The Login Screen 6
2.4 Log on with the Web Interface 7
2.5 The Welcome Screen 8
3 Options in the Menu Bar 9
3.1 Outgoing Mails 10
3.2 Spam Mails 11
3.2.1 Spam Mail Options 11
3.3 CISS Queue 12
3.4 Archive 2.0 14
3.4.1 Overview of the User Console (GUI) 14
3.4.2 Performing an Archive Search 14
3.4.2.1 The Simple Search 15
3.4.3 Show History 20
3.4.4 Category Voting 21
3.4.5 Audit Session 23
3.4.6 Categories 26
3.4.7 Results Window 26
3.4.8 Show message: 28
3.4.9 Suggest for or Assign to Category 30
3.5 MailSealer 31
3.6 User Settings 32
3.6.1 User Profile 32
3.6.2 E-Mail Aliases 33
3.6.3 Filter Lists 35
3.7 Logoff 37
4 The REDDOXX Outlook AddIn 37
4.1 Installation of the Outlook AddIn 38
4.2 Outlook AddIn Menu Overview 41
Image: Reddoxx Logon Button Image: Reddoxx Folder 41
4.3 REDDOXX Logon 42
4.4 The REDDOXX Menu 43
4.5 Message Archiving 44
4.6 Blacklist an e-mail manually 46
5 Glossary 48

1 Introduction and Start

To access the REDDOXX Appliance, there are different user interfaces from which the user can choose.

1. REDDOXX User Console
2. REDDOXX Outlook Add-In
3. REDDOXX Web Interface

All of these options provide the user the same function set and a consistent Look & Feel. Differences between the interfaces will be marked in the corresponding chapter of this user manual with a symbol and described in further detail.

1.1 REDDOXX User Console (User GUI)

The REDDOXX **U**ser **C**onsole is a portable program file with the extension named <.exe>. It will not be installed, but executed with a double click on the program. This software can be downloaded from the REDDOXX Support Center. There is also a <.msi> version available to distribute the program in the network.

1.2 REDDOXX Outlook AddIn

The REDDOXX Outlook AddIn is a Windows-DLL which is integrated into Microsoft Outlook with the AddIn technology. The AddIn is loaded within the start up of Outlook. If a specific REDDOXX function is used for the first time after loading Outlook, a login is required. The AddIn only supports Outlook versions 2002 - 2007 and only in combination with MS Exchange Server. The installation and some special features of the Outlook-AddIn are described at the end of this document in chapter 4. In principle, Outlook 2000 works fine, but with minor restrictions in the context menu of a mail which are not supported by REDDOXX.

1.3 REDDOXX Web Interface

The REDDOXX Web Interface (**WI**) is provided by the Appliance itself. You only need a common web browser to access your emails. Insert following address into your web browser bar:

http://<IP-Address-or-Hostname-of-the-Appliance>
https://<IP-Address-or-Hostname-of-the-Appliance> (encrypted)

2 Login

For safety reasons, the REDDOXX Appliance is only accessible via a login. Therefore you have to authenticate yourself as follows with a vaild user name and password.

2.1 Login with the User Console

UC

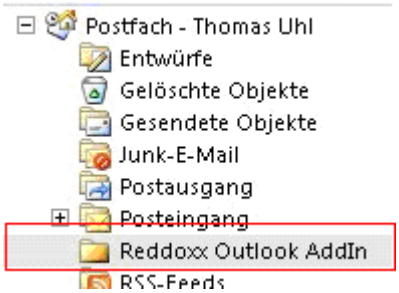
Start the user console by double clicking on the file *rdxuser.exe*. The login window appears. Continue with Step 3 in the login window.

2.2 Login with MS Outlook

Outlook Add-In

Prerequisite:
Reddoxx Outlook AddIn needs to be installed on the user's computer.

1. Start MS Outlook.
   In the tool bar, a REDDOXX button is shown. Additionally, you will see a new folder below your post box named *Reddoxx Outlook AddIn*.

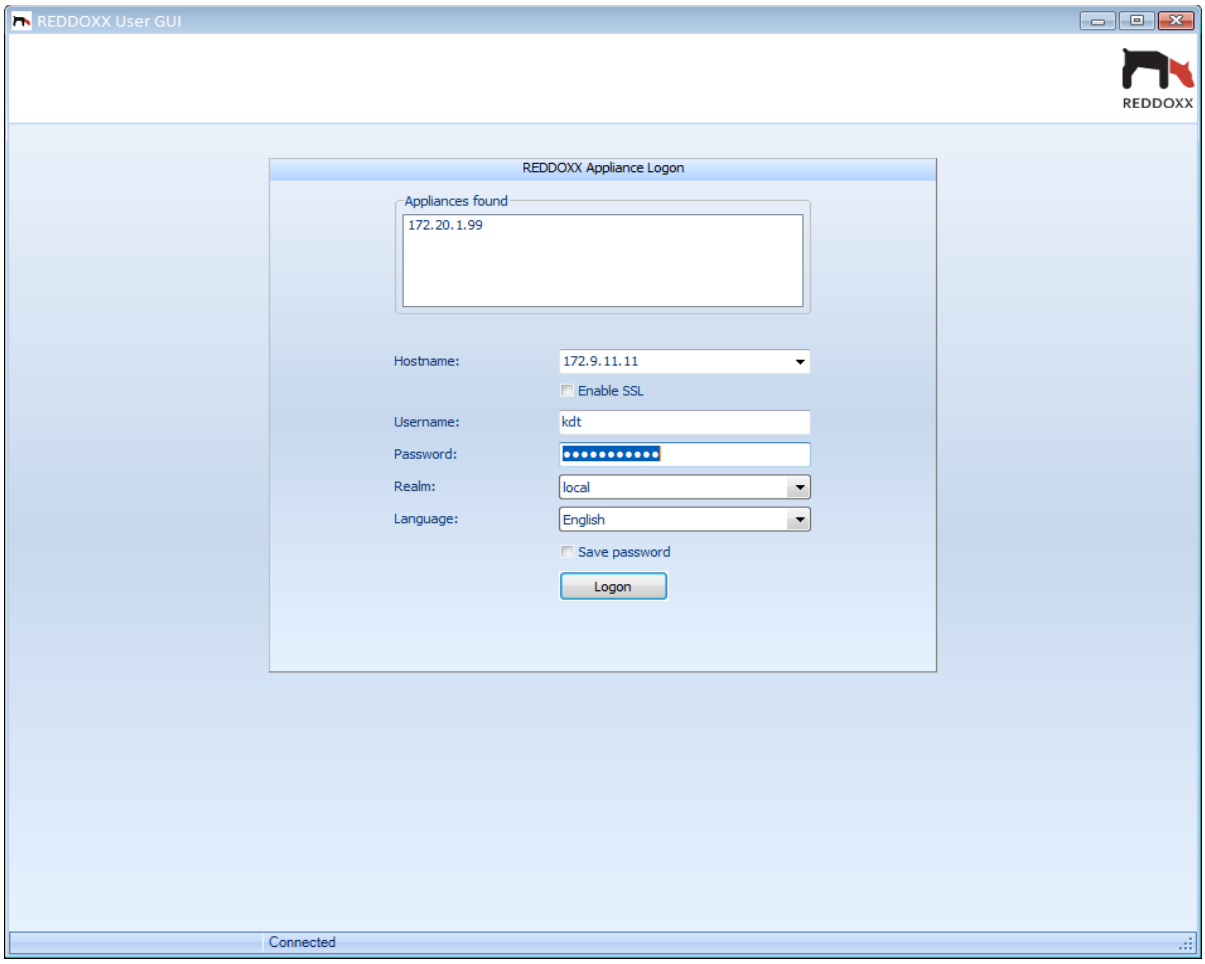


2. Click the REDDOXX button or click the Reddoxx Outlook AddIn folder to log in.

The log in window will appear. Continue with step 3.

2.3 The Login Screen

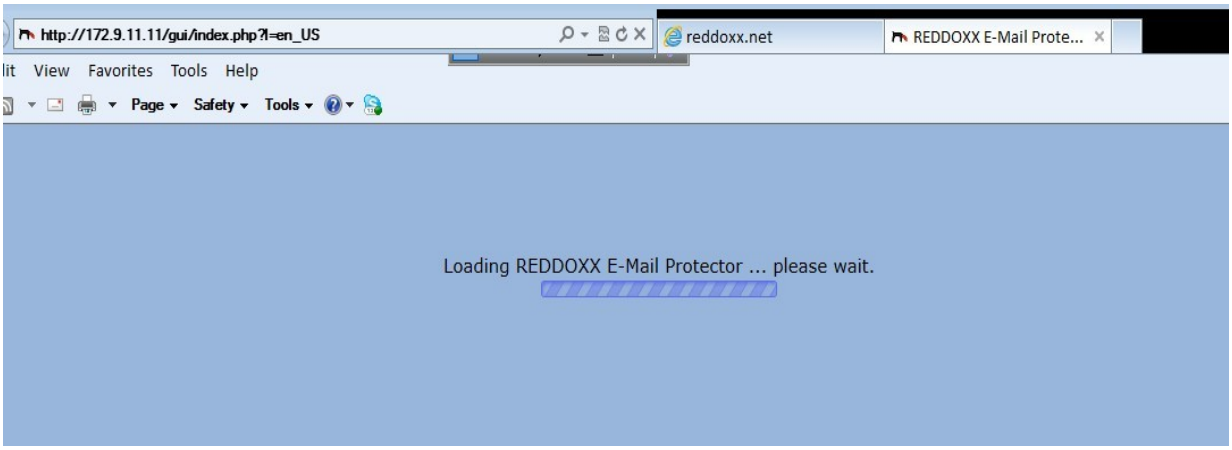
The software automatically searches for existing Appliances inside your local network. In the field "***Appliances found***", all detected Appliances are listed.



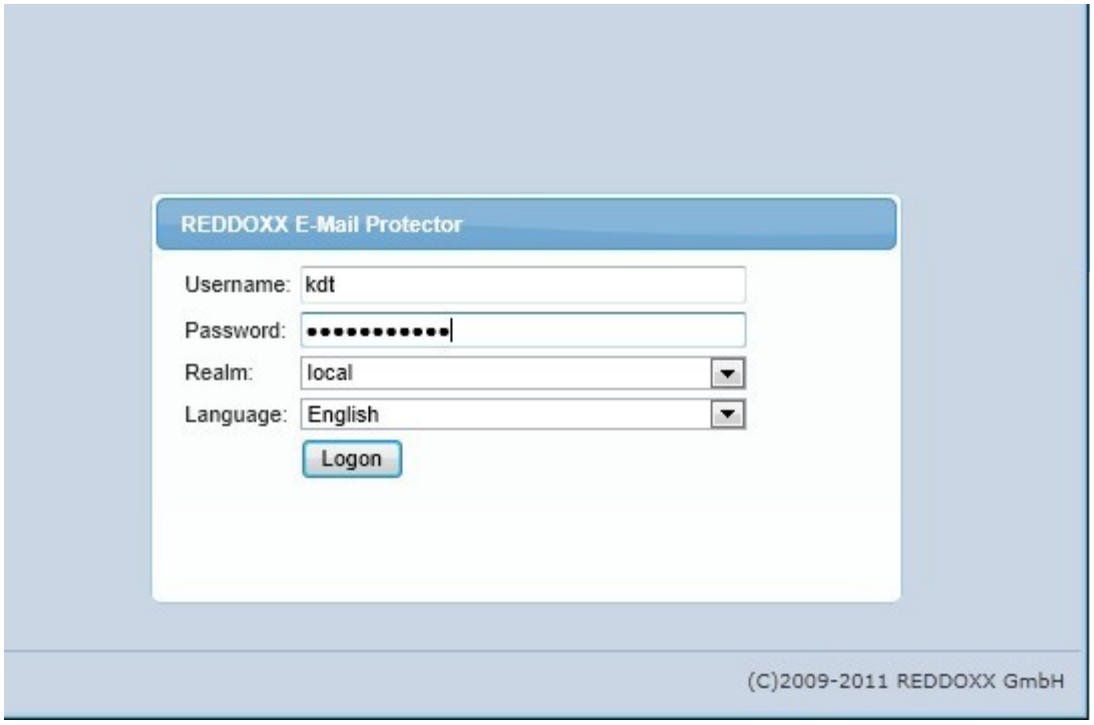
1. **Hostname**: Choose the hostname or IP address from the field „Appliance found". With a double click, the appliance will be inserted automatically into the field "hostname". You can also manually insert a hostname or the IP address of your Appliance into this field. (Contact your administrator if you don't know it).
2. **Username**: Enter your user name.
3. **Password**: Enter your password.
4. **Realm**: Select the option „local" or the realm to which you belong. The realm is a section similar to a domain in which you have to authenticate yourself.
5. **Language**: Choose the desired language in the selection list. The selection contains the currently installed languages English and German.
6. **Save Password**: The password will be kept for the next login to enable auto login.
7. **Logon**: Click LOGON. Continue with the welcome screen.

2.4 Log on with the Web Interface

WI In the web browser address bar, or URL bar, enter the IP address or the hostname of the REDDOXX appliance. A new window will open in your browser...



After loading, the login window will appear.



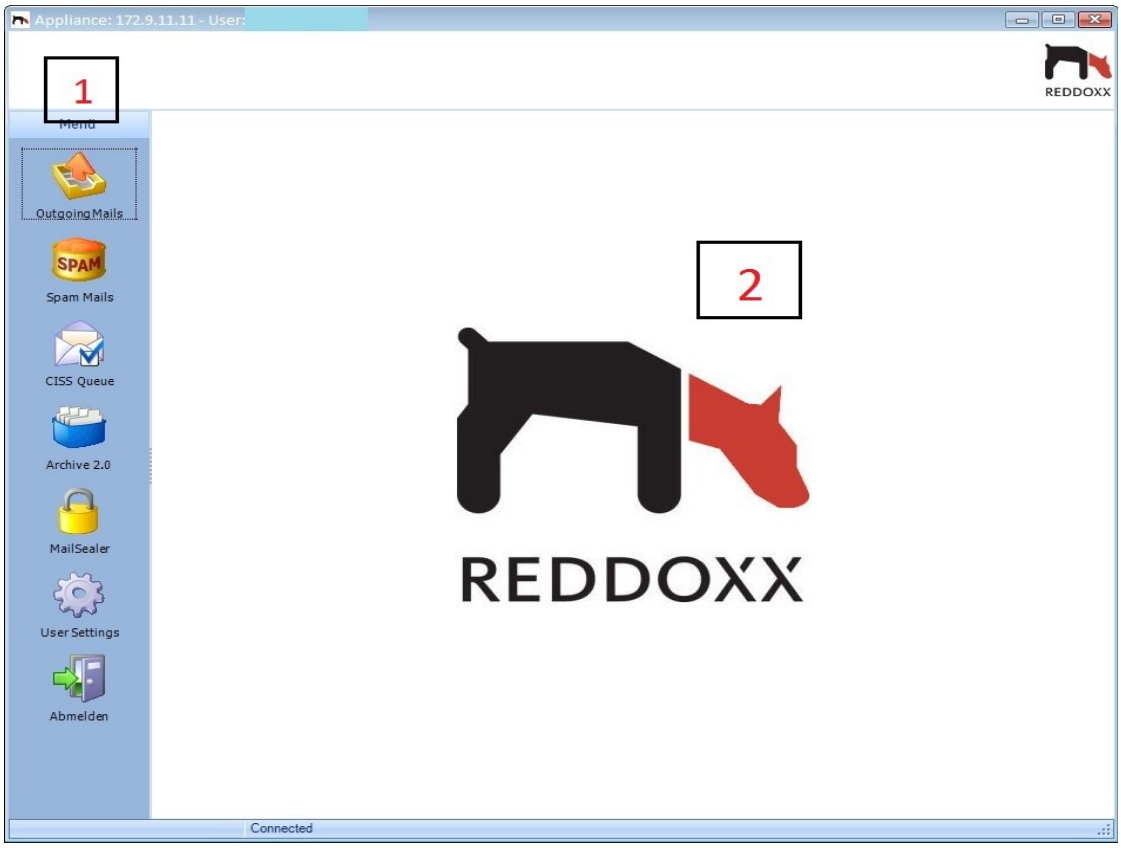
1. Enter your username and password in the respective fields.
2. Choose “local” in the realm field, unless your are authorized for a specific realm. A realm, similar to a domain, is an area in which the user authenticates him/herself.
3. Select the language in which you would like the GUI to be displayed. There is a choice between German and English. Click “Logon” when you are ready to proceed. The Welcome Screen opens.

2.5 The Welcome Screen

UC

The following welcome screen will appear after a successful login.

WI



Legend: 1. Menu Bar 2. Display Window

Outlook Add-In

3 Options in the Menu Bar

The main menu consists of access to the following options: Outgoing Mails, Spam, CISS Queue, Archive 2.0, MailSealer, User Settings, and Logoff.

Outgoing Mails
Here you see all mails listed which the user is sending to the internet.

Spam Mails

Here is listed all mails which were sent to the user, but were detected as spam.

CISS Queue

The CISS Queue contains all mails which have not yet been released by the sender or by the recipient.

Archive 2.0

In the MailDepot, the user will have access to all mails which have been archived by the appliance.

MailSealer

The MailSealer (Light) offers the user the possibility to send mails encrypted with a password.

User Settings

The user settings allow the user to change the general settings. The user maintains their email addresses here.

Logoff

Log off from the personal user GUI.

3.1 Outgoing Mails

All mails scheduled to be sent by the Appliance will first land in the Outgoing Mails Queue. The Outgoing Mails section displays these mails.
If the mail could not be sent immediately due to a failure on the recipient's side or to a network failure, your Appliance attempts to resend the mail in regular intervals. After an approximate 1.5 hours delay, the sender receives the first notification that the mail could not be delivered up to this point. The '*Last Result*' column informs you of the cause of the failure.

If the failure has been corrected, but you do not wish to wait for the next send cycle, you can manually send the respective mail by right-clicking on it. It is possible to select multiple mails at once.

If the delivery of the mail is not at all possible, for example, due to a misspelling in the domain name of the mail address, you can delete the mail by right-clicking on it. However, a mail which cannot be delivered within a period of 5 days will be deleted automatically from the Outgoing E-Mails Queue. The sender will receive a notification regarding this action.

Find: You can search for specific mails in the Outgoing Mails Queue, as well as delete mails listed in the queue. In the list view, you can see the ID, the time the mail was received, the sender of the mail, it's recipient, and the size of the mail. You can also sort the mails by their criteria here. To do so, please click on the column heading.

In: Restrict the search by either searching for the *sender* or the *recipient* of the mail.

Queue: You can choose between **SMTP** and **POP3**.

In the **SMTP Queue** are mails which have not yet been sent. In the **POP3 Queue** are mails which have been collected from the in-boxes, but have not yet been validated by the REDDOXX appliance. The mails are then waiting for the next retrieval through the e-mail client program.

3.2 Spam Mails

Mails found in the Spam Mails Queue have been classified as spam mail by the Spamfinder filters defined on the appliance. In case mails have been falsely recognized as spam (False Positive), the user can deliver them to the recipient manually.

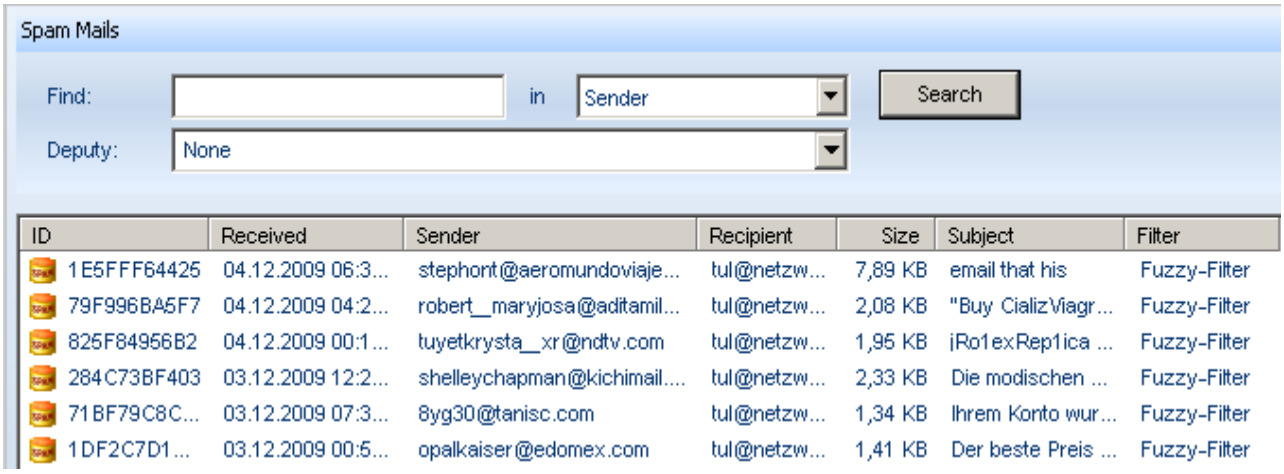

Spam Mails
Find:
in
Sender
Search
Deputy:
None
ID
Received
Sender
Recipient
Size
Subject
Filter
1E5FFF64425 04.12.2009 06:3... stephont@aeromundoviaje... tul@netzw... 7,89 KB email that his Fuzzy-Filter
79F996BA5F7 04.12.2009 04:2... robert_maryjosa@aditamil... tul@netzw... 2,08 KB "Buy CializViagr... Fuzzy-Filter
825F84956B2 04.12.2009 00:1... tuyetkrysta_xr@ndtv.com tul@netzw... 1,95 KB ¡Ro1exRep1ica ... Fuzzy-Filter
284C73BF403 03.12.2009 12:2... shelleychapman@kichimail.... tul@netzw... 2,33 KB Die modischen ... Fuzzy-Filter
71BF79C8C... 03.12.2009 07:3... 8yg30@tanisc.com tul@netzw... 1,34 KB Ihrem Konto wur... Fuzzy-Filter
1DF2C7D1... 03.12.2009 00:5... opalkaiser@edomex.com tul@netzw... 1,41 KB Der beste Preis ... Fuzzy-Filter

Image: Spam Mails Queue

Find: You can search for specific mails in the Spam Mails Queue, as well as delete mails listed there. In the list view, you can see the ID, the time the mail has been received, the sender of the mail, it's recipient, and the size of the mail. You can also sort the mails by their criteria, here. To do so, please click on the column heading.

In: Restrict the search by searching for either the *sender* or the *recipient* of the mail.

Deputy: Please select the e-mail address whose queue you are allowed to manage as a deputy from the deputy list. Via the *Settings* section you can determine a deputy who is supposed to substitute your own queues then.

3.2.1 Spam Mail Options

You have certain options to process the spam mail afterwards. Right click on a selected spam mail to open the context menu.

Deliver:

The mail will be delivered immediately.

Deliver (Whitelist Address):

The mail will be delivered immediately and added to the address white list.

Deliver (Whitelist Domain):

The mail will be delivered immediately and the sender's domain name will be added to the domain white list.

Delete

Spam mails will be deleted automatically from the Spam Mails Queue after a period of 60 days. However, you can manually delete specific or multiple emails from the queue. To do so, right click on the mail you want to delete and select the '*Delete*' option from the context menu.

Preview

A preview of your mail allows you to first preview your spam mail before you decide to deliver or delete the mail.

3.3 CISS Queue

When using the CISS filter, the sender receives an e-mail which must be acknowledged, so that his/her mail to the REDDOXX user can be sent. The mail remains in the CISS queue until it is confirmed. You can browse the CISS queue if you are waiting for a certain mail and you can permanently bypass the filter by adding the sender's address.

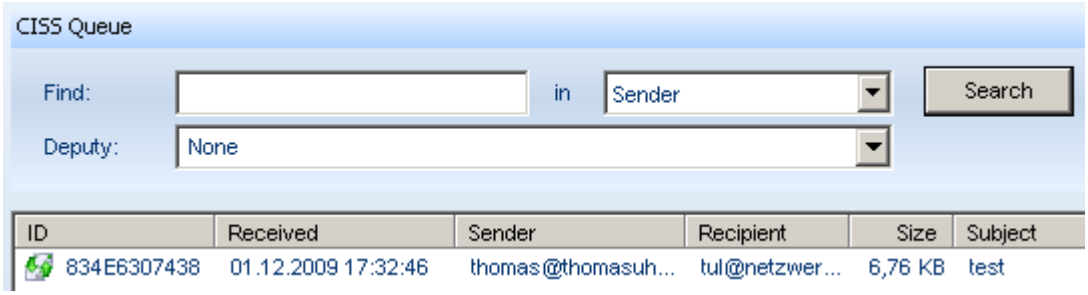


Image: Search CISS queue

The search, deliver, delete, and preview options are consistent with those of the spam mail options.

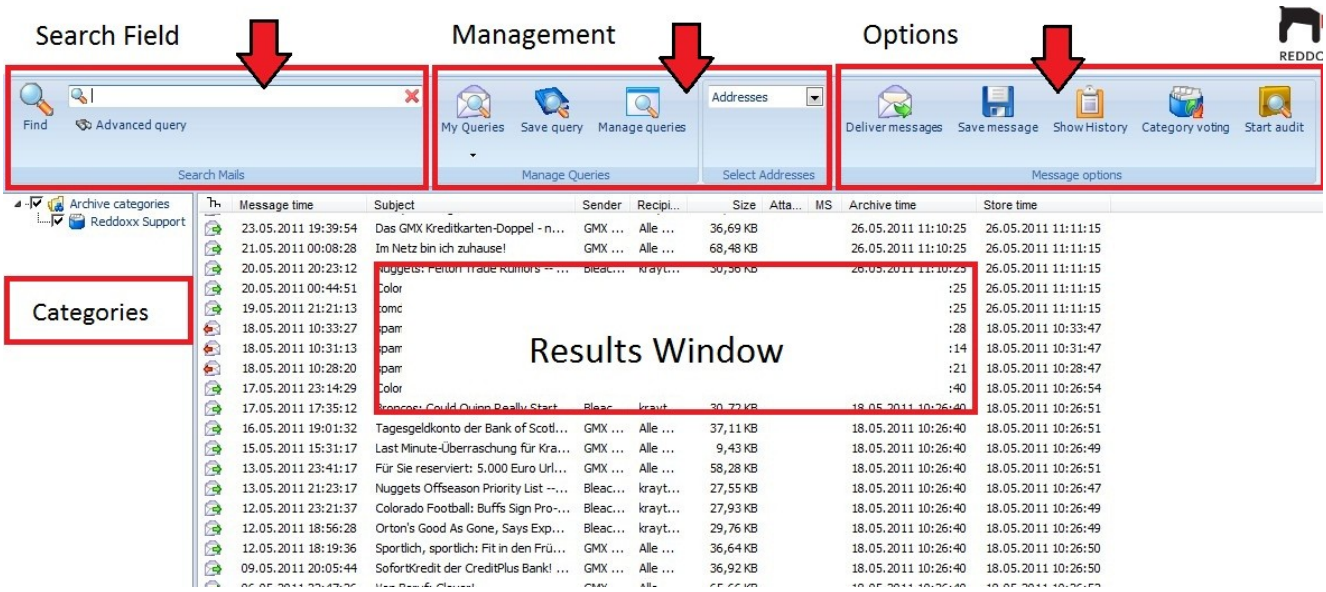
NOTICE

Mails (for example, newsletters), which have not been confirmed by the sender, can be released by the REDDOXX user manually.

3.4 Archive 2.0

All mails which are received or sent through the REDDOXX Appliance are saved to the archive, and also those mails which meet the policies defined by the REDDOXX administrator. In the archive, you have the capability to search for specific mails through defined criteria, and are able to redeliver the mails to your mailbox. All mails found belonging to the user in the archive, can be displayed in the archive window where further actions can be taken on a mail.

3.4.1 Overview of the User Console (GUI)



Overview of the User Console

3.4.2 Performing an Archive Search

The search function in the archive is based on a full-text index. This means that upon reception, the mails, including attachments, is immediately searched for individual text patterns and these patterns are then catalogued and noted for future reference. When a future search is performed, only the index will be searched, leading to a faster search result.

NOTICE

The following file formats are supported for full-text indexing:

All text-based documents and files.

Also note that embedded images inside a PDF documents, a fax for example, cannot be found using a full-text search.

3.4.2.1 The Simple Search

A simple search (or standard search) allows the user the possibility to search the archive for incoming and outgoing mails quickly and efficiently.

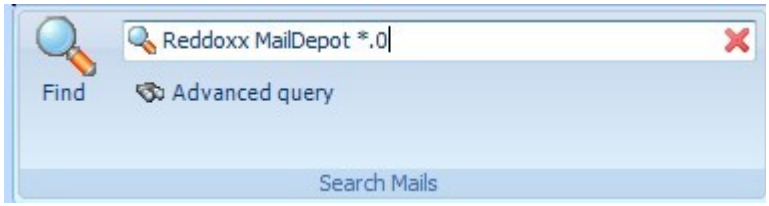


Image: Simple Search Field

Search terms input

Enter one or more search keywords (or parts thereof), which should be found in the contents of a mail (AND function). An OR-function search needs to be performed in the "*Advanced query*" section.

Wildcard Characters

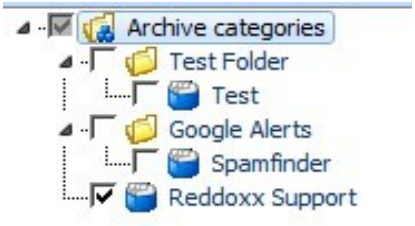
The input of a wildcard character is allowed in the middle or at the end of a word, but not at the beginning of a word.

- * (Star) Any desired number of characters will be observed.(also none)
- ? (Question Mark) Exactly one desired character.

Fields and Contents included in the search

Different fields and contents (including the attachments) are searched when a query is performed. The fields related to the mail, for example the creation date, sender, recipient, all recipients included in the cc field, are included in the search. If a search needs to be more detailed and individual fields need to be included, then perform the search in the "*Advanced query*".

Search in Categories

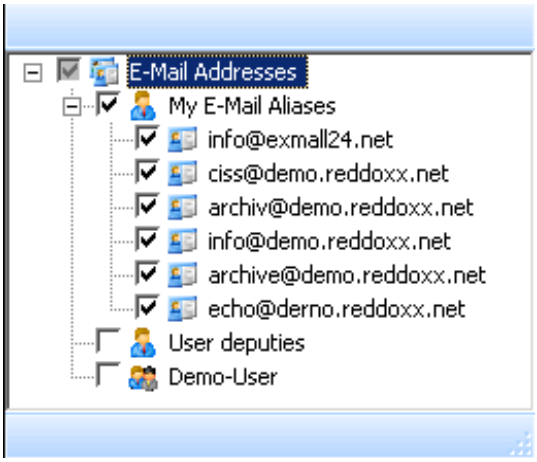


Categories are defined groups of mails meeting certain criteria established by the REDDOXX administrator. By selecting a category from the displayed category list, the user can limit the query to one specific category. If a category is not specified, the entire archive will be searched.

.

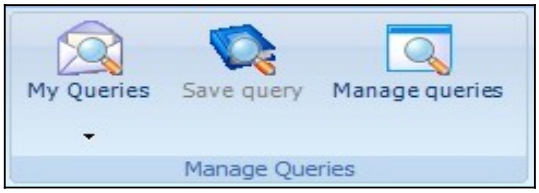
Search Limitations using addresses

By default, the addresses used in a query, are those which are assigned to the user whom is currently logged on to the user console. (My E-Mail Aliases)



Addresses for which the user acts as a deputy need to be selected in order to be included in any searches.

Manage Queries:

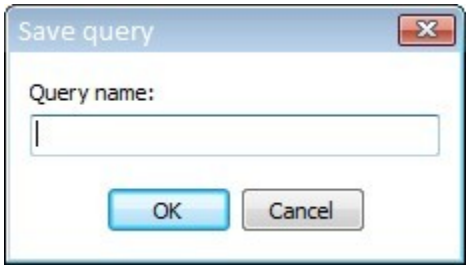


Individual searches can be saved under "*Manage Queries*" to be used again at a later date or which can be changed to better optimize the given search.

My Queries:

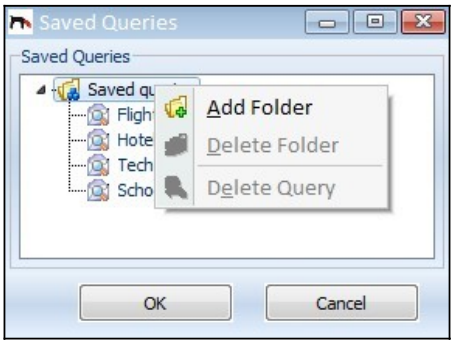
Under "*My Queries*", the user can view previous searches that have been saved and activate the query to run immediately.

Save query:

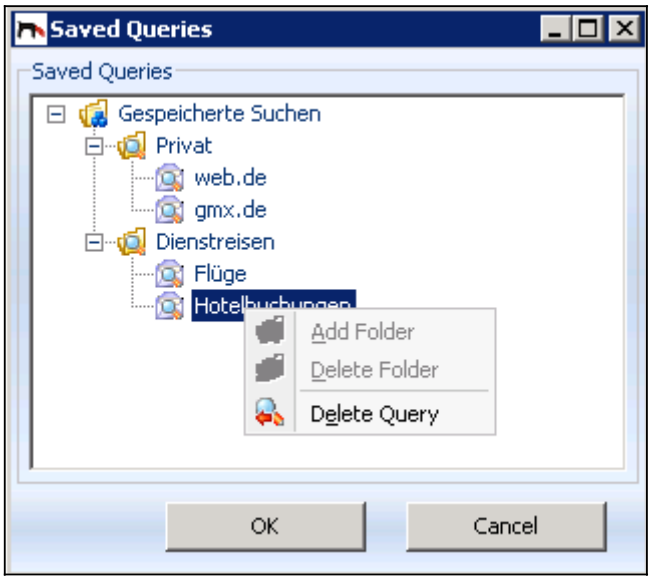


If the same query is routinely performed, the user can save it here and give the query a name to be saved under "*My Queries*".

Saved Queries:

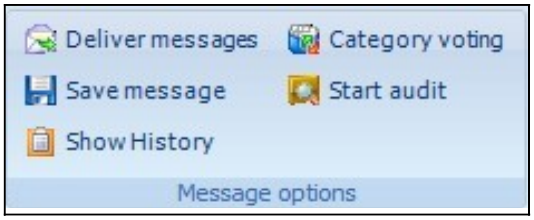


Under "*Saved Queries*", the user can add folders to help organize their saved searches.



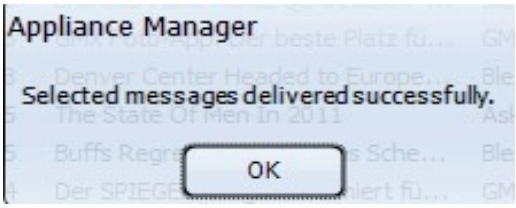
By clicking on "*Manage Queries*", the user can add a folder according to its search contents or delete an existing folder or query.

Message Options



In "*Message Options*", the user can choose from 5 different actions to further process a mail.

Deliver messages:

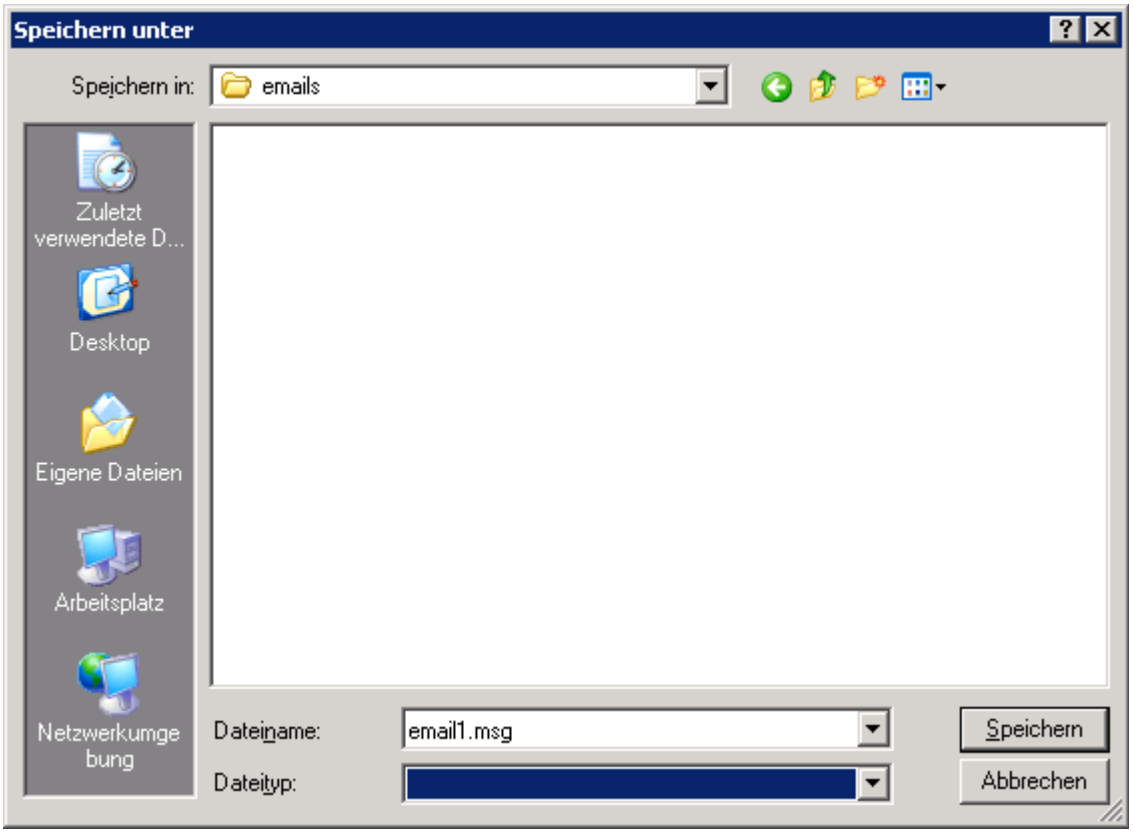


By selecting this action, the mail will be resent to the recipient.

NOTICE

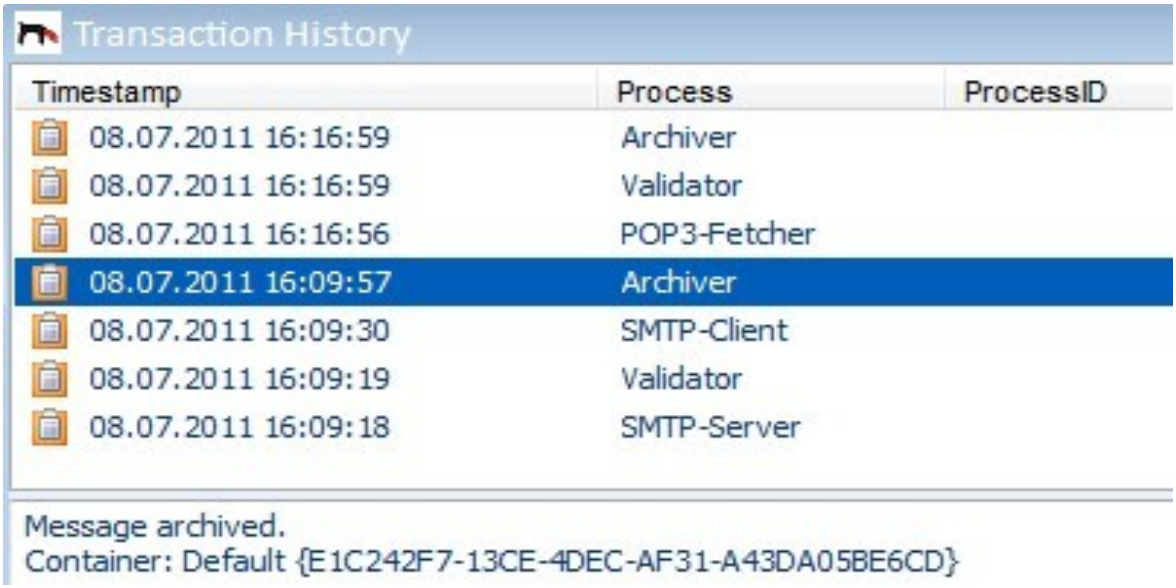
Mails imported via MSX-Agent will be delivered to the recipient as an .msg attachment..

Save Message



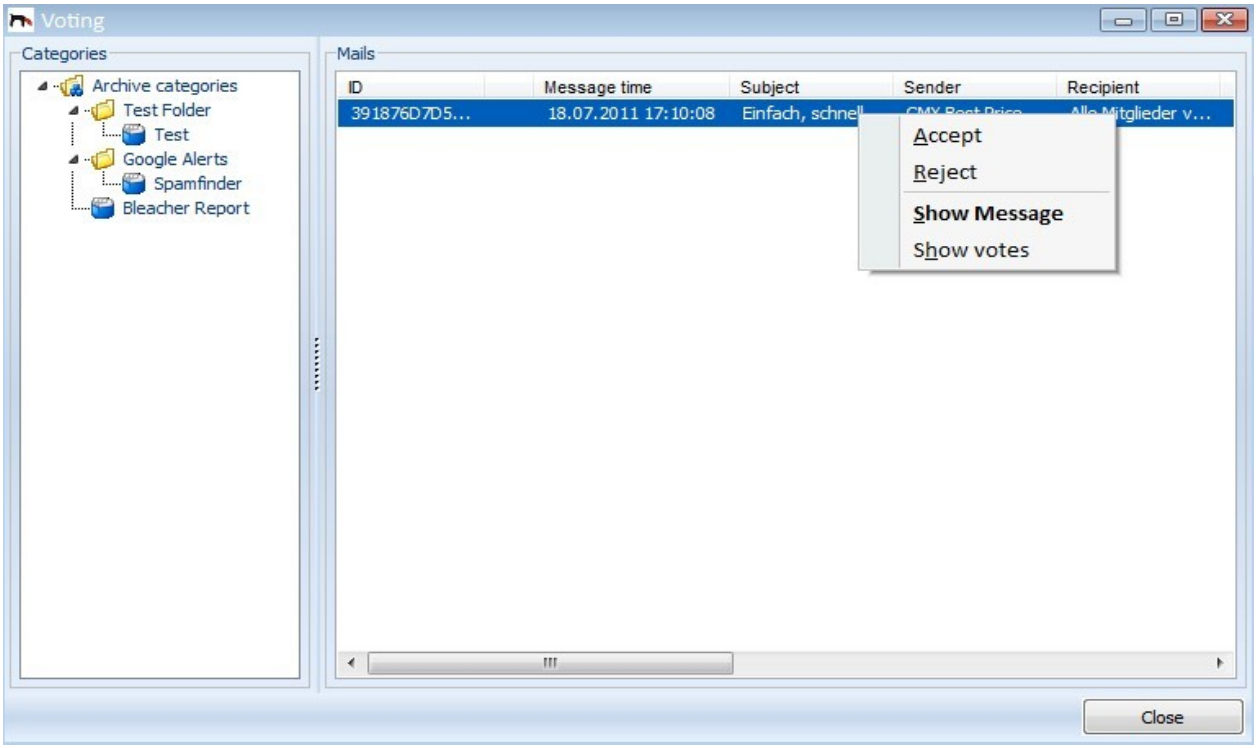
By selecting this action, the mail will be saved in .msg format to a chosen file with a corresponding name in the network.

3.4.3 Show History



By selecting this option, the user can choose to view the technical history of a mail. By clicking on an individual process, the user can view the logged details more closely.

3.4.4 Category Voting



A user, provided the user is a qualified controller in the category, can accept or reject a category suggestion from other users under “Category Voting”. The user can also see a preview of the suggestion, as well as view the current vote count.

For more details about the “Category Voting” function, please follow this link to our Administrator Manual on the REDDOXX Support homepage:

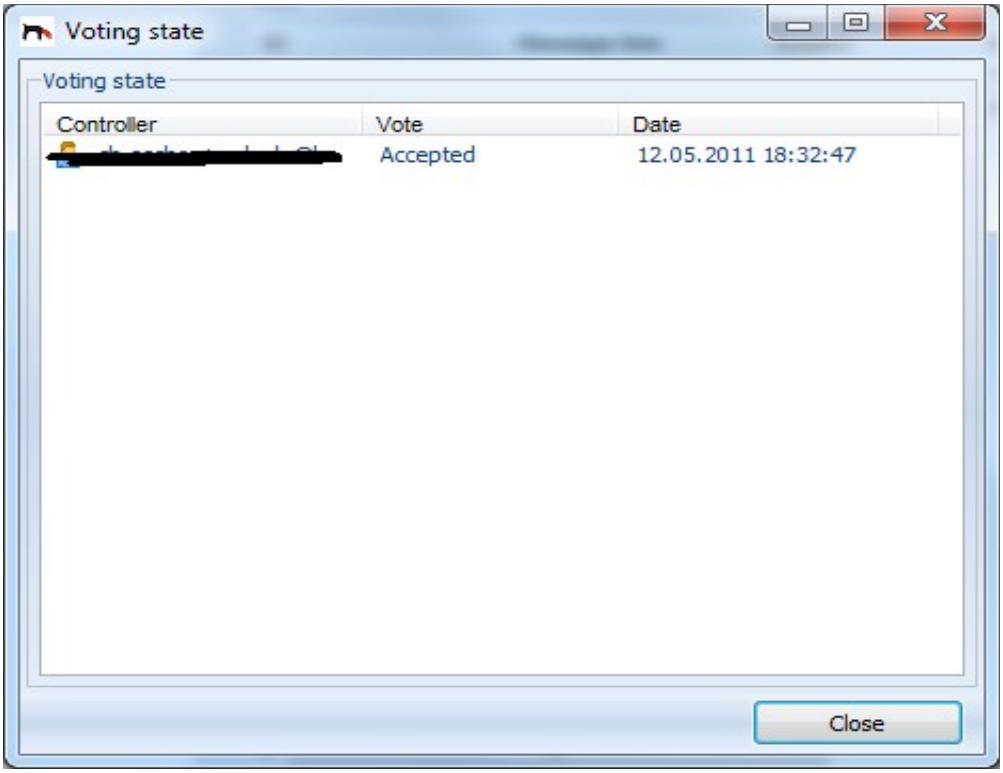
http://support.reddoxx.net/manual/admin2027en/#__RefHeading__27531_2087378751

Accept: The suggestion to include this mail in the respective category is accepted.

Reject: The suggestion to include this mail in the respective category is rejected.

Show message: The message will be displayed in a separate window.

Show Votes:

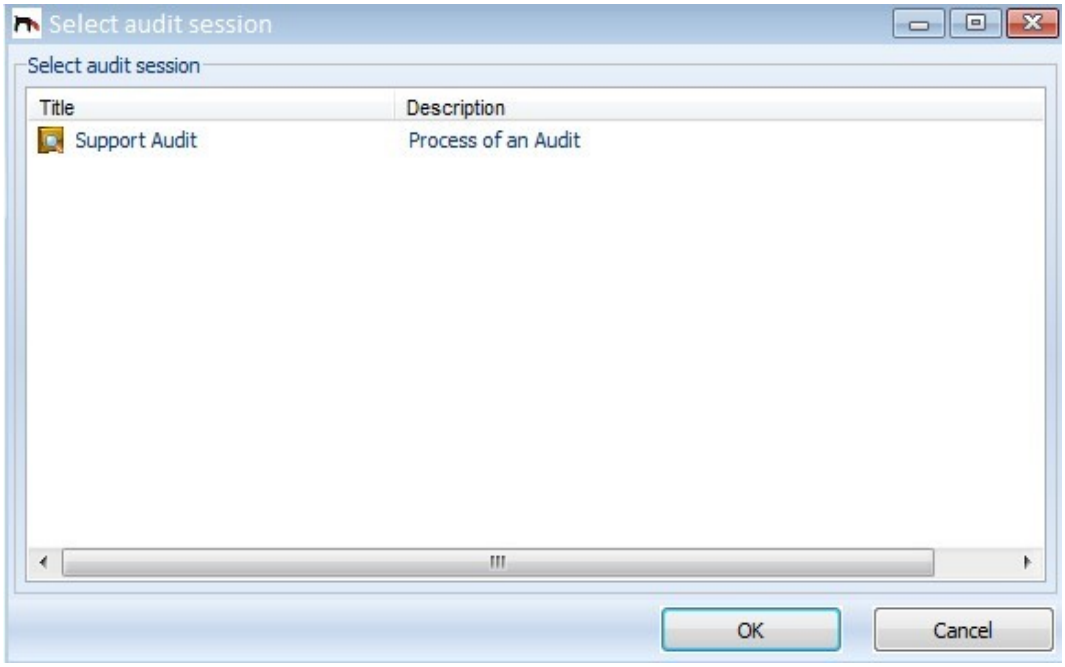


The current voting results will be displayed.

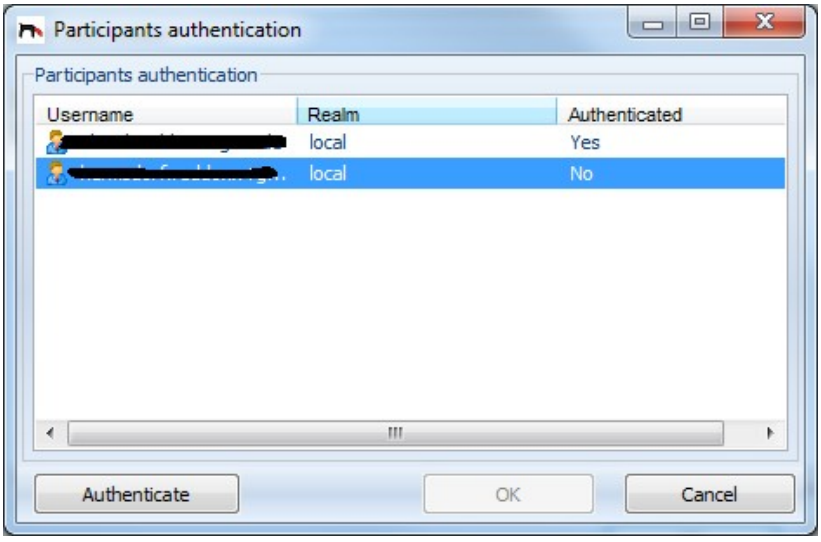
3.4.5 Audit Session

An Audit Session (Revision, Examination) allows authorized users access to selected mails. An audit session is coordinated for a limited time by an administrator. The authorized user, or auditor, is able to access the audit session from their user console. An audit is completely detailed, in order to show who, when, and where a mail was accessed and on whose authority the audit session was ordered.

Start Audit

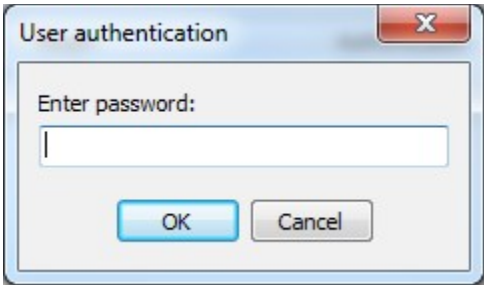


The audit sessions currently available will be displayed in the window. Choose the audit which should be performed. Confirm the selection in the following pop-up window.



The audit will not begin until all participants have been successfully authorized for the audit session. When all participants have been successfully authorized, the “OK” button can be selected.

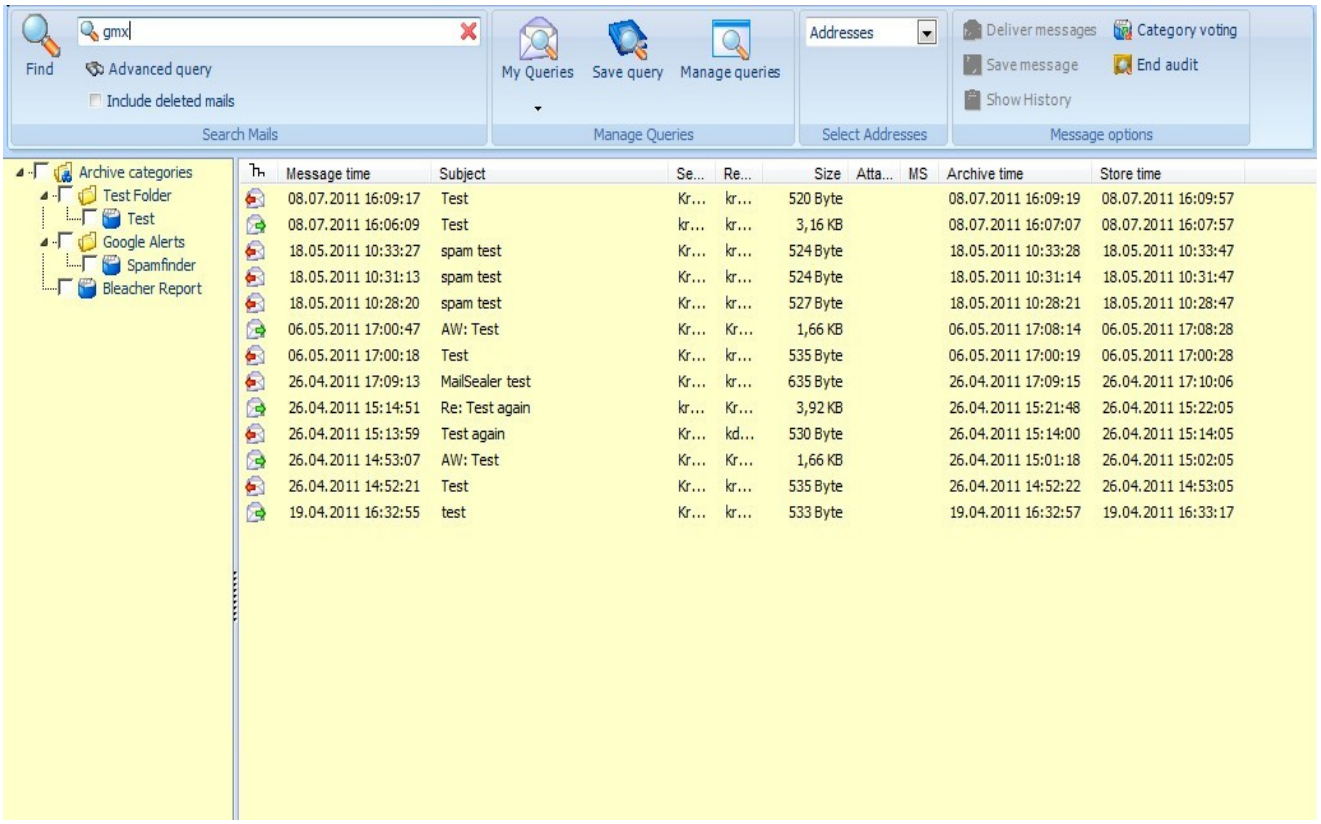
All participating users need to authenticate themselves by entering their password.



Entering your user password is required before the audit session can begin.

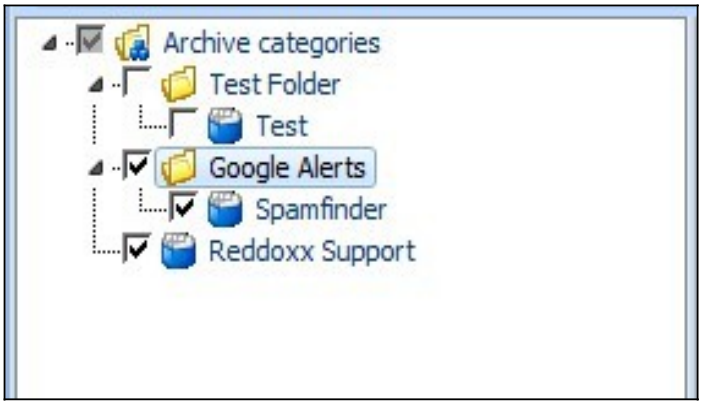
A pop-up window acknowledging the successful authorization of the user will appear next.

The audit session will now begin. An audit session can be recognized by its yellow background.



By clicking on “End Audit” in the upper right hand corner, the user console display will return to its normal layout.

3.4.6 Categories



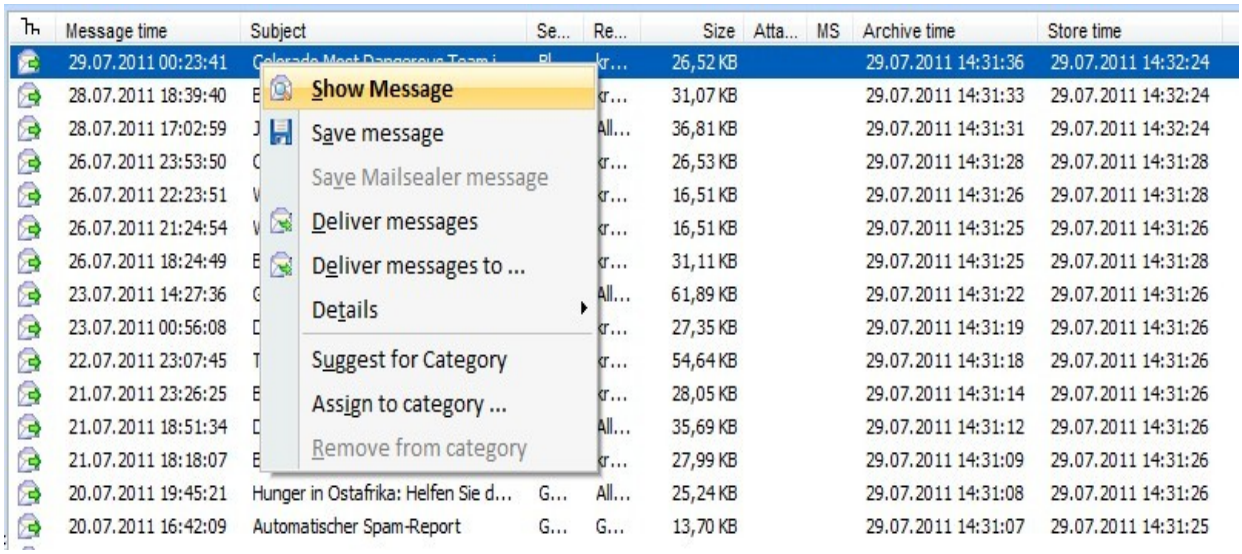
The categories defined by the administrator will be displayed for every user, as long as the respective user has the necessary access rights to view the category. Categories make the overview of the archive easier for the administrator and the users. If so configured, mails found in certain containers can be made available through the category. Users do not have the authority to create categories.

For further information to category creation and administration, follow this link to our Administrator Manual on the REDDOXX Support homepage:

http://support.reddoxx.net/manual/admin2027en/#__RefHeading__27531_2087378751

A double click on a category will allow the user to view all messages found under the category. Searching in a category can be found in this handbook under Chap. 3.4.2.1.

3.4.7 Results Window



The mails meeting the criteria given in a query, by selecting a category, or which meet the display time will be shown in the “Results Window”.

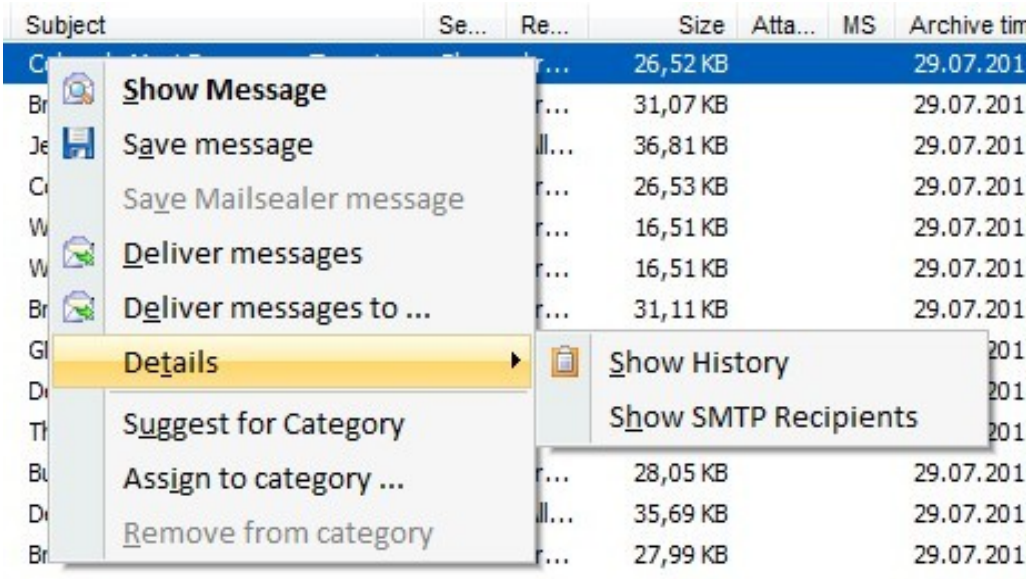
Incoming Mails: Mails marked with a green arrow are classified as incoming mails. An incoming mail is defined as a message coming from an external sender addressed to an internal domain.

Outgoing Mails: Mails marked with a red arrow are classified as outgoing mails. An outgoing mail is defined as a message sent from an internal domain (a trusted network) to an external recipient.

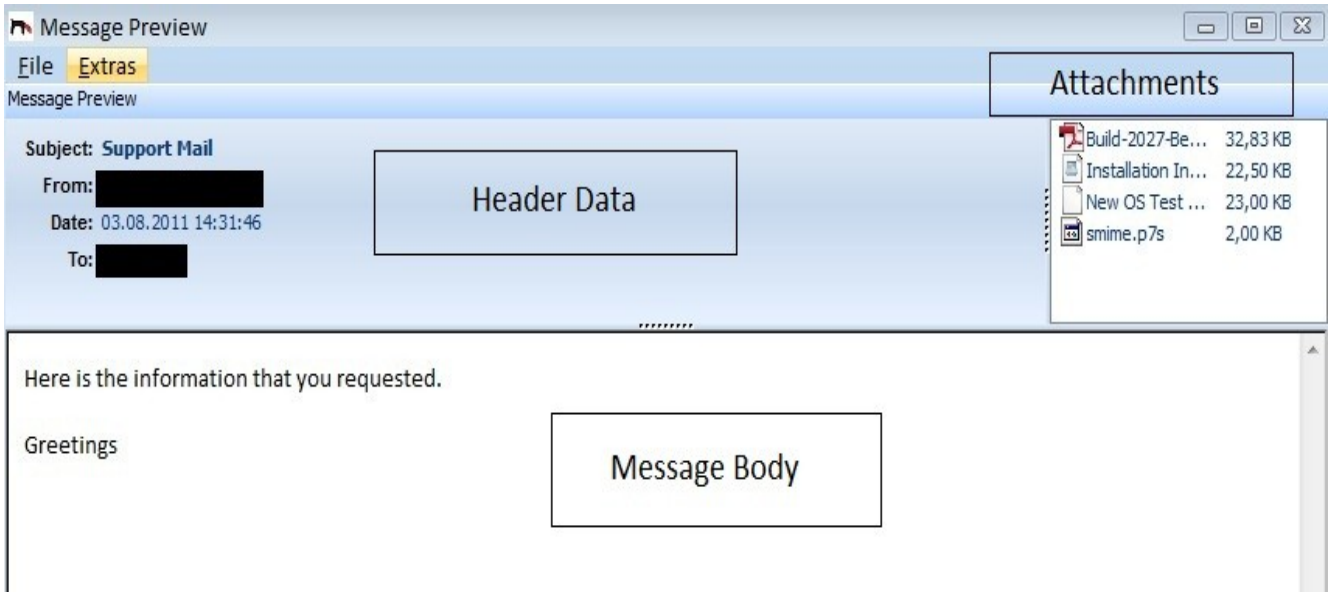
MSX Agent Mails: Mails imported through the MSX Agent are marked with an envelope.

MS Outlook Mails: Mails imported through the OutlookAddIn are marked with a Microsoft Outlook symbol.

By right clicking on a mail in the list, the user will be presented with the following options.



3.4.8 Show message:



File: Close the message preview.

Extras: Save or deliver the message. For further information, see Chap. 3.4.2.3 in this handbook.

Header Data: Here you find the most important data of the header of the message.

Attachments: Here the user can see the attachments found which were attached to the message. By right clicking on an attachment, the user can choose from the following:

Open: Opens the respective attachment. In order to successfully open the attachment, the correct software for the format of the attachment needs to be available on the host computer.

Open with: Opens the attachment. The user can choose with which software the attachment should be opened.

Save attachment: The attachment can be saved to a file in the network.

Message Body: The contents of the message will be displayed in this field.

Save message: Explained in Chap. 3.4.2.3.

Save MailSealer Message

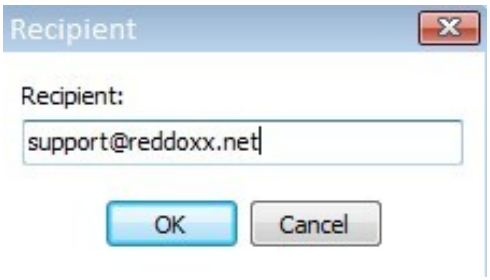
An encrypted mail will be saved unencrypted. The method is the same as you would under “Save Message”.

Deliver message

Explainer in Chap. 3.4.2.3.

Deliver Message to

The recipient of a message can be entered.

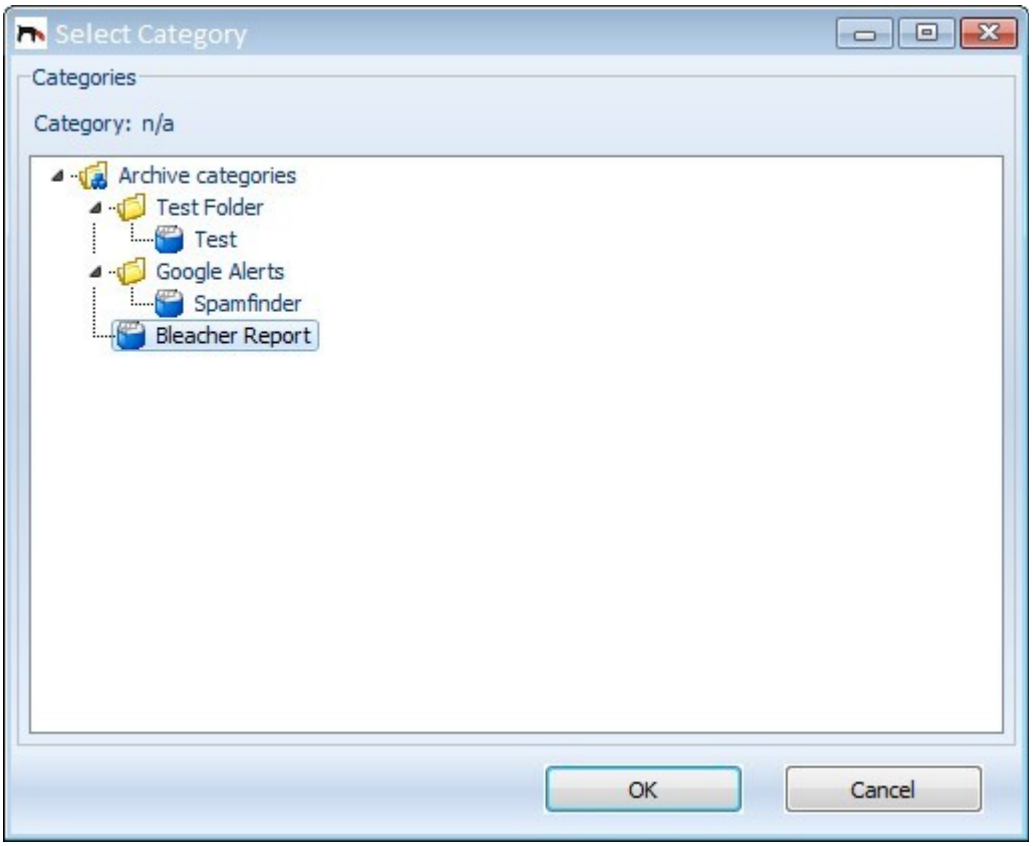


Details

Show history: Explained in Chap. 3.4.2.3.

Show SMTP recipients: The recipients of this message will be shown.

3.4.9 Suggest for or Assign to Category



Suggest for Category:

The category for which the mail should be suggested can be chosen here. The user needs to have the correct access rights to suggest a mail for a category.

Assign to Category:

The category to which the mail should be assigned can be made here. The user needs to have the correct access rights to assign a mail to a category.

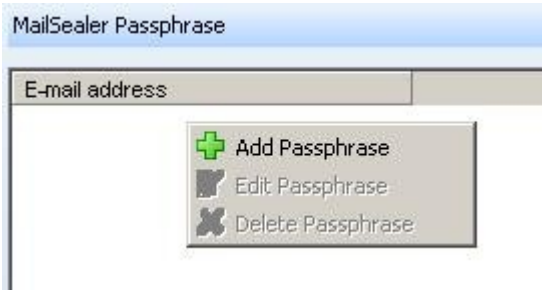
3.5 MailSealer

With the integrated REDDOXX MailSealer, you are able to encrypt your mails quickly and simply. An encryption strength of 256 bit AES is used for encryption purposes.

Add a Passphrase

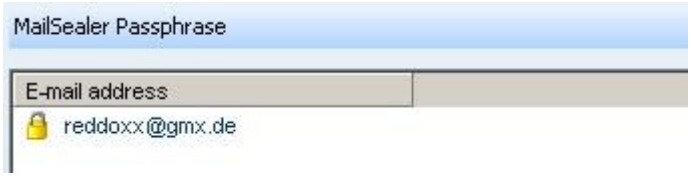
If you would like to encrypt the entire mail traffic directed to a specific e-mail address, you proceed as follows:

Right click in the list. Select *'Add Passphrase*' from the context menu.



Enter the respective e-mail addresses and the corresponding passphrases. If you want to apply the encryption immediately, check the *'Active*' box.

All mails being sent to the e-mail address configured will be encrypted automatically.



Edit Passphrase

In the future, if you would like to send e-mails to a specific address unencrypted, you proceed as follows:

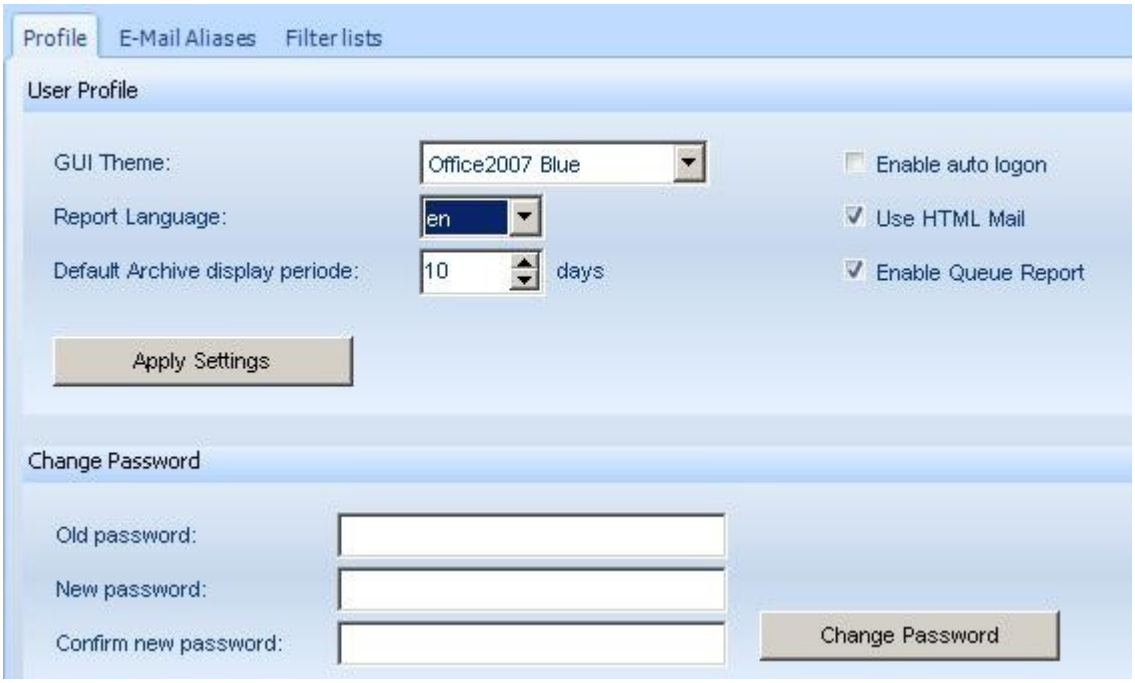
Right click on the e-mail address you want to edit and select the '*Edit Passphrase*' option from the context menu.

Clear the '*Active*' box and confirm with '*Save*'.

3.6 User Settings

In the User Settings section, you can adjust your user profile, your e-mail address, the settings for your daily queue report, the layout of the Appliance Manager, as well as change your password.

3.6.1 User Profile



GUI Theme: Select a skin for your Appliance Manager.

Report Language: Select the language for your daily queue report. You can choose between English and German.

Default Archive display period:

Initially the archive list shows the mails which have been archived within the specified time period. A longer time period can be looked up at any time using the search function.

Enable auto logon:

Allows the user to log on to the Appliance Manager automatically, without typing in the password again. The password is stored on the Appliance.

Use HTML Mail: Check this box if you want to receive the queue report in HTML format.

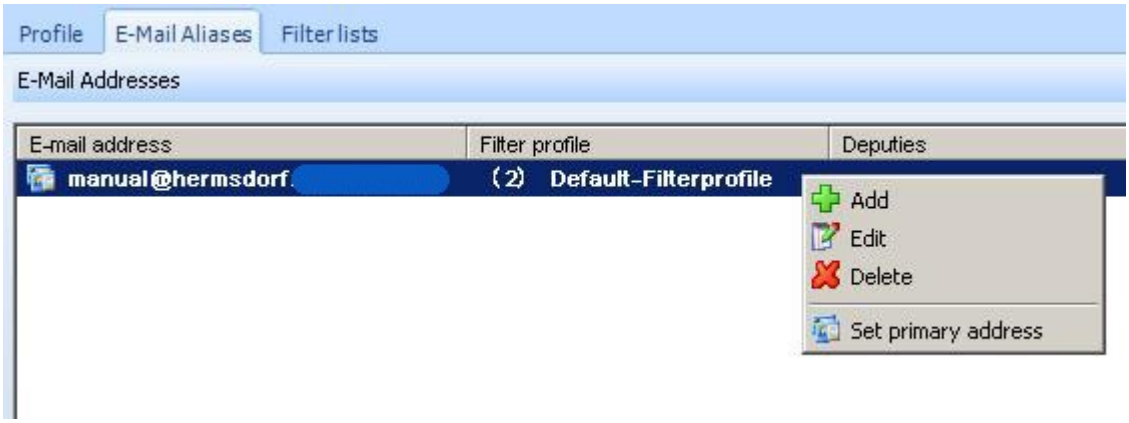
Enable Queue Report:

Check this box if you want to receive the queue report, including a list of spam mails, on a scheduled basis.

Change Password: Here you can change the login password. Specify your old and your new password, and click the '*Change password*' button.

3.6.2 E-Mail Aliases

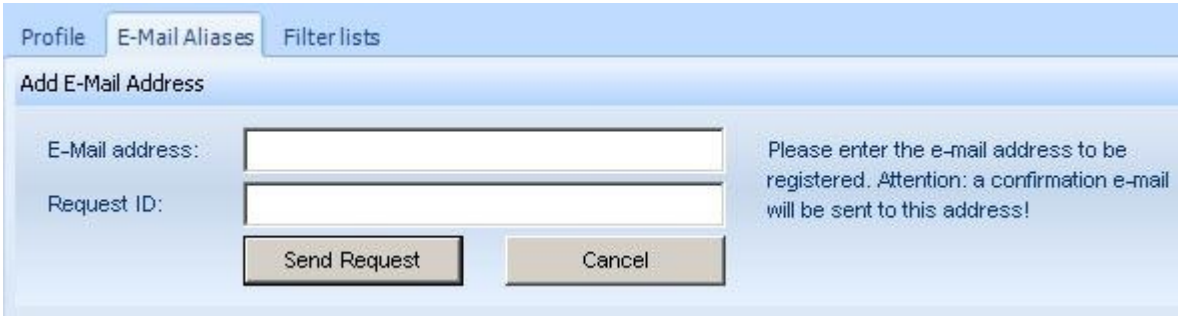
E-mail aliases are e-mail addresses which are assigned to a specific user. This user can manage all e-mail addresses that are assigned to him/her. In the management section, you can activate the filtering of spam per e-mail address (default) as well as define a deputy for your own e-mail address.



Add a new E-Mail Alias

Since the Appliance recognizes new e-mail addresses automatically, it is not necessary to add new e-mail aliases manually. If you want to prevent the filtering for a specific e-mail address, you need to add a new e-mail alias manually. If you do not add it manually, and wait instead for the Appliance to recognize the new e-mail address automatically, the filtering of this address will be carried out instantly. To add e-mail aliases manually please proceed as follows:

Right click in the list and select '*Add*' from the following context menu.



E-Mail address:
Enter the new e-mail address and click on '*Send Request*'. You will then receive an e-mail at this address.

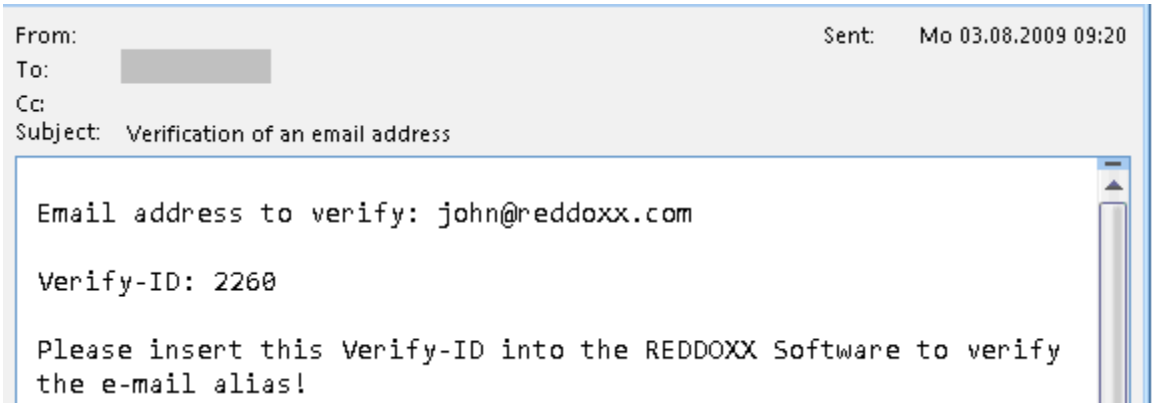

From:
Sent: Mo 03.08.2009 09:20
To:
Cc:
Subject: Verification of an email address
Email address to verify: john@reddoxx.com
Verify-ID: 2260
Please insert this Verify-ID into the REDDOXX Software to verify the e-mail alias!

Image: Verification E-Mail

Request-ID: To prevent third parties from accessing the new e-mail address, a security check is necessary. Please enter the Verify ID that you find in the mail which you have received from the Appliance, and click on 'S*end ID*'.

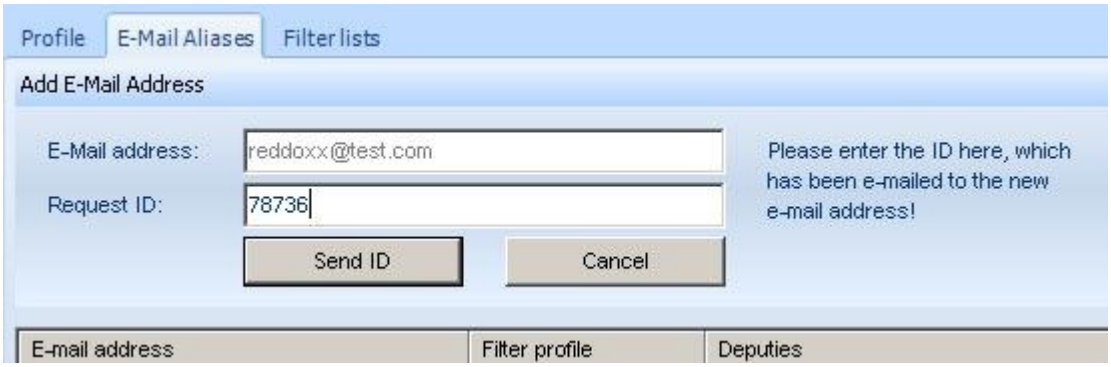


Image: Verification of the new E-Mail Alias using the Verify ID

You can activate or deactivate the filters for your e-mail alias. Furthermore, you can define deputies, so that other users can manage the queues of this e-mail alias under their account.

Double-click an e-mail alias in the list to edit the settings.

Image: Edit E-Mail Alias

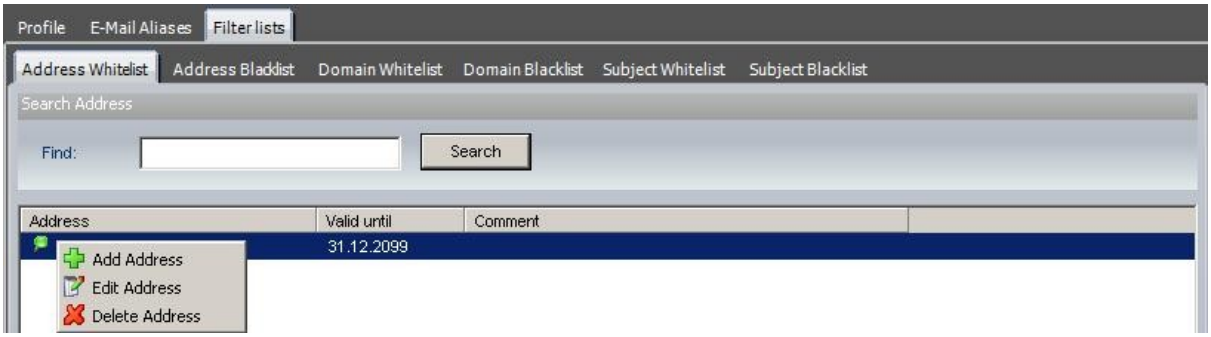
Deputy: Select a user from the list of deputies who should be allowed to manage this e-mail address. The deputy can then access the spam queue and the archive.

Profile: From the *Profile* field you can also select '*No Profile*'. Mails sent to this address are not filtered any longer. After an automatic recreation of an e-mail alias, this alias will always be assigned the *Default Profile*.

Click '*Save*' to finish editing the settings. The changes are instantly active.

3.6.3 Filter Lists

In the filter lists, it is possible to set addresses, domains, and subjects to trusted and untrusted.

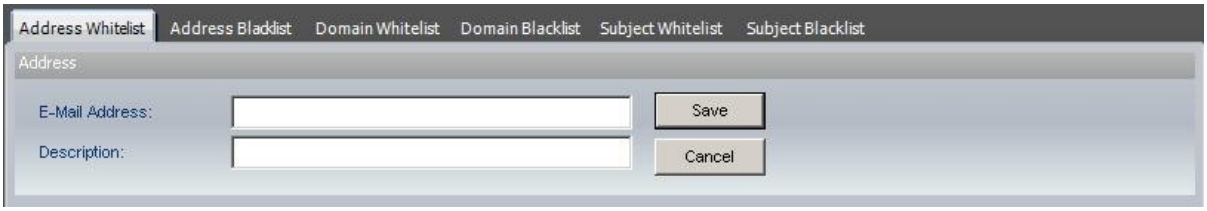


There are different types of filter lists to choose from:

Address Whitelist:	E-mail address is trusted.
Address Blacklist:	E-mail address is untrusted.
Domain Whitelist:	E-mail domain is trusted.
Domain Blacklist:	E-mail domain is untrusted.
Subject Whitelist:	E-mails with this subject are trusted.
Subject Blacklist:	E-mails with this subject are untrusted.

You can add, edit, and delete whitelist- and blacklist entries.

Add Whitelist



E-mail address: Add the e-mail address of a trusted sender.

Description: A description can be given.

Add blacklist

Email address: Add the e-mail address of the sender you want to block.

Description: A description can be given for this entry.

Action: Which action should be performed if the above given address matches.

There are 3 types of actions from which to choose:

Quarantine: The e-mail will be moved to the quarantine list.

Tag: The e-mail will be delivered to the recipient with a flag in the subject line.

Decline: The e-mail will not be accepted from REDDOXX. Therefore a non-delivery e-mail is sent back.

Valid until: The validity of this entry is defined.

NOTICE

Domain and subject filter lists are configured with the same procedure.

3.7 Logoff

By clicking the '*Logoff*' symbol, the connection to the Appliance will be closed. The Login window appears in order you to be able to log in again or also under another username.

4 The REDDOXX Outlook AddIn

The REDDOXX Outlook AddIn integrates the REDDOXX user console with MS Outlook. It is launched with the start of MS Outlook. The main difference to the user console or the web interface is the ability to archive mails from your mailbox directly to the REDDOXX MailDepot. Furthermore, there is a feature which allows the user to add a spam sender to the blacklist. Most of the feature sets are the same as the feature of the user console.

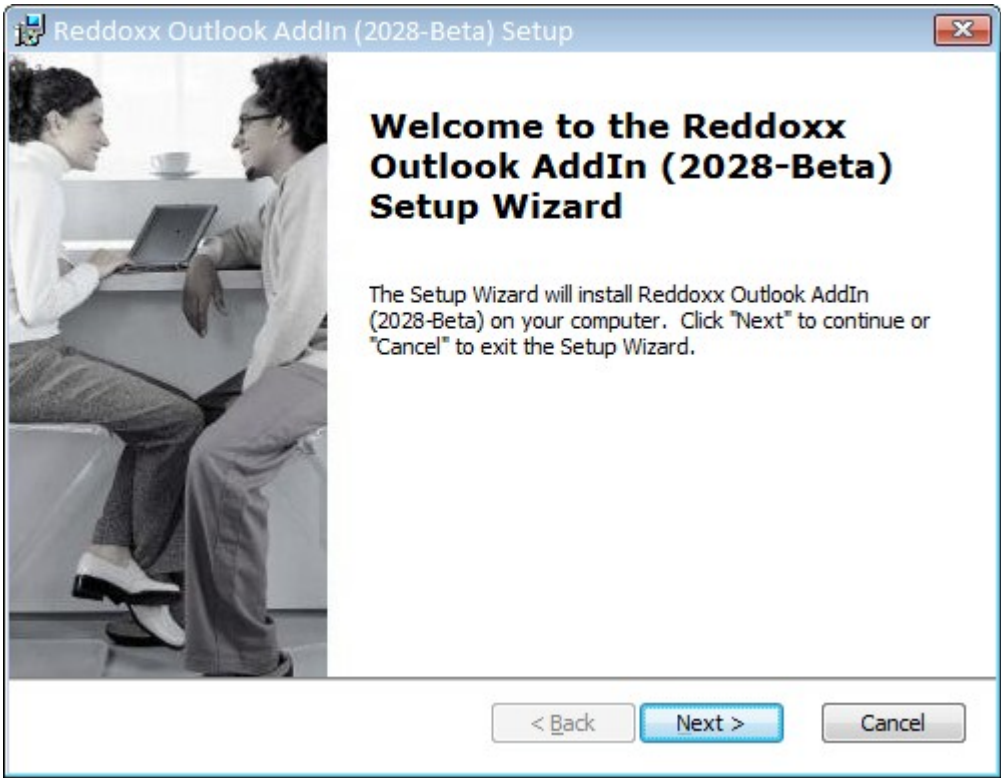
NOTICE

The Reddoxx Outlook AddIn is supports only MS Outlook. Other mail clients such as Outlook Express, Lotus Notes or Thunderbird are not supported.

4.1 Installation of the Outlook AddIn

1. **Download** the setup file under the URL:
   http://support.reddoxx.net/downloads.php

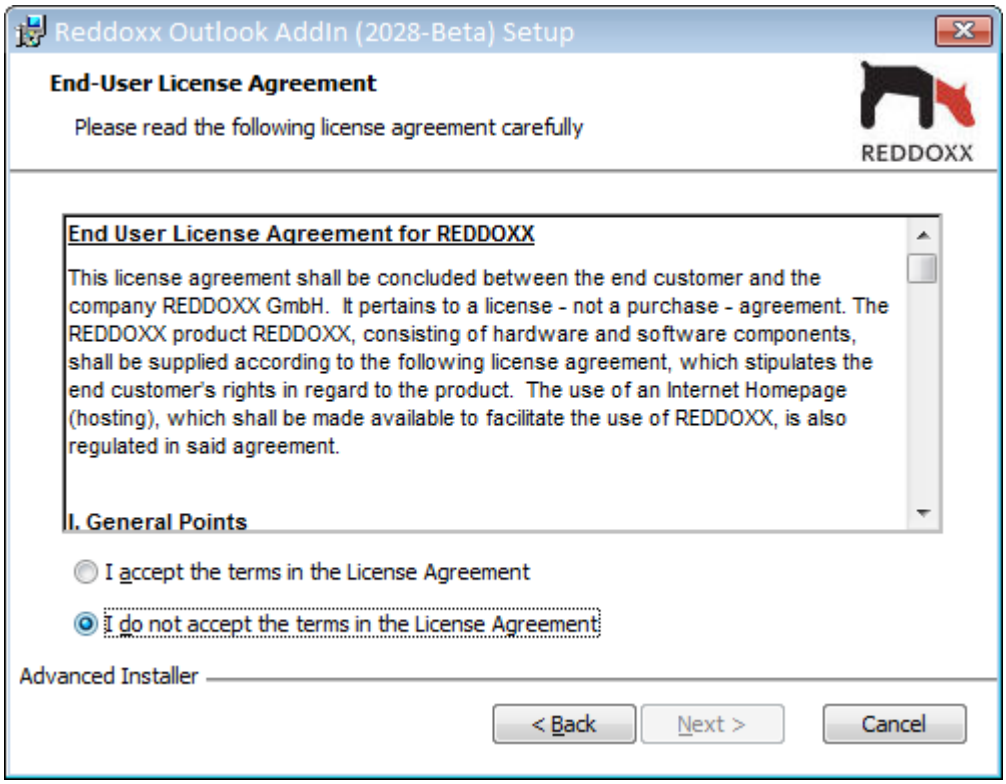
2. **Launch** the setup with a double click on the <.msi> file. A welcome screen appears.


Reddoxx Outlook AddIn (2028-Beta) Setup
Welcome to the Reddoxx Outlook AddIn (2028-Beta) Setup Wizard
The Setup Wizard will install Reddoxx Outlook AddIn (2028-Beta) on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.
< Back
Next >
Cancel

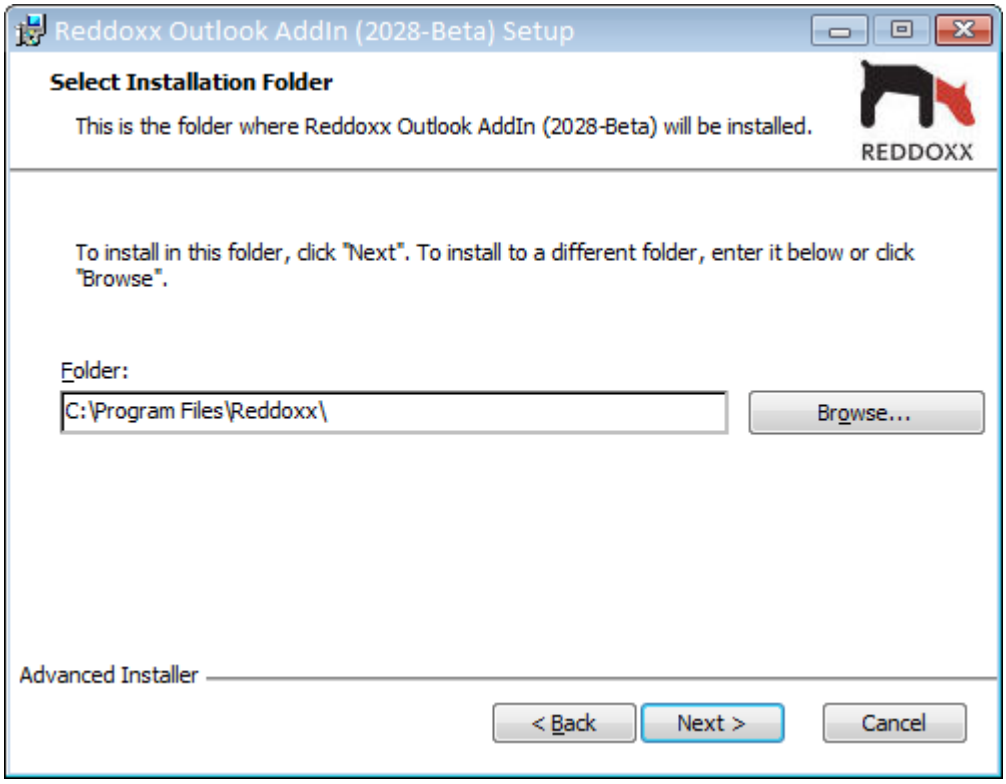
3. Continue by clicking “**Next**”.

NOTICE

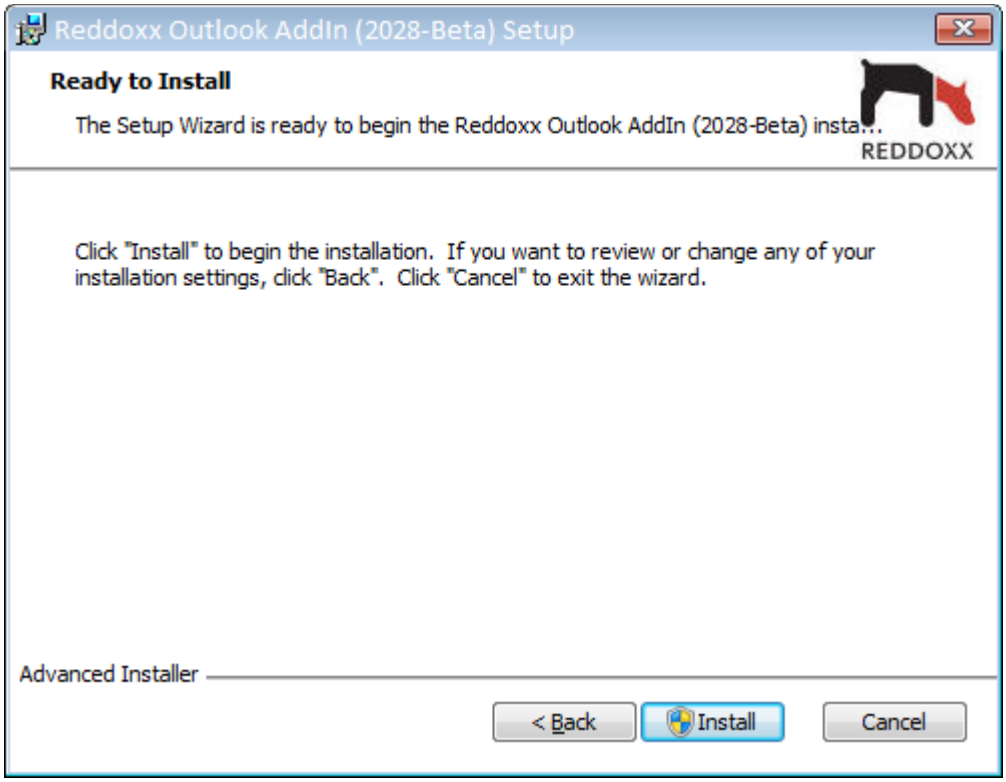
MS Outlook must be closed before beginning the setup. Make sure the MS Outlook process is not listed in the task manager process list.


Reddoxx Outlook AddIn (2028-Beta) Setup
End-User License Agreement
Please read the following license agreement carefully
REDDOXX
End User License Agreement for REDDOXX
This license agreement shall be concluded between the end customer and the company REDDOXX GmbH. It pertains to a license - not a purchase - agreement. The REDDOXX product REDDOXX, consisting of hardware and software components, shall be supplied according to the following license agreement, which stipulates the end customer's rights in regard to the product. The use of an Internet Homepage (hosting), which shall be made available to facilitate the use of REDDOXX, is also regulated in said agreement.
I. General Points
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Advanced Installer
< Back
Next >
Cancel

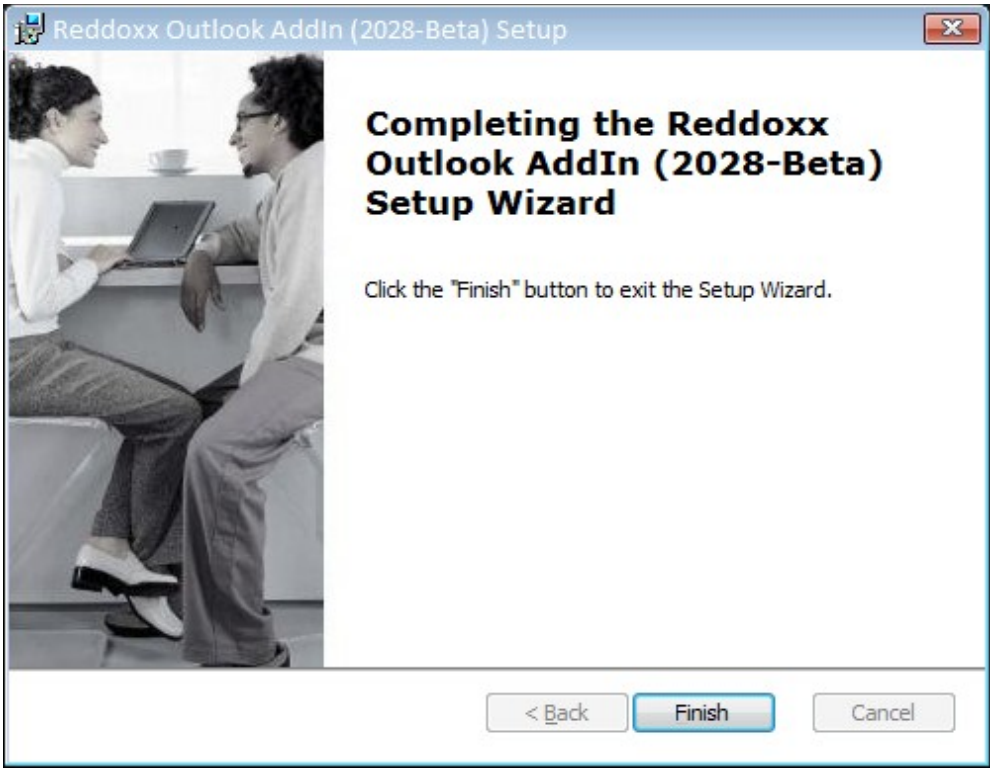
4. Read the end user license agreement and click on “**Next**“ if you agree to the terms.


Reddoxx Outlook AddIn (2028-Beta) Setup
Select Installation Folder
This is the folder where Reddoxx Outlook AddIn (2028-Beta) will be installed.
REDDOXX
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files\Reddoxx\
Browse...
Advanced Installer
< Back
Next >
Cancel

5. Choose an installation folder of your choice and continue with “**Next**“.


Reddoxx Outlook AddIn (2028-Beta) Setup
Ready to Install
The Setup Wizard is ready to begin the Reddoxx Outlook AddIn (2028-Beta) insta...
REDDOXX
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced Installer
< Back
Install
Cancel

6. The Setup Wizard is ready to install. Click on “**Install**“ to start the installation.


Reddoxx Outlook AddIn (2028-Beta) Setup
Completing the Reddoxx Outlook AddIn (2028-Beta) Setup Wizard
Click the "Finish" button to exit the Setup Wizard.
< Back
Finish
Cancel

7. The installation has finished. Click on „**Finish**“ to exit the set-up process.
8. You may now launch MS Outlook.

4.2 Outlook AddIn Menu Overview

After launching MS Outlook, a REDDOXX button appears in the symbol bar. Additionally, you can see in your mail box navigation tree a new folder named Reddoxx Outlook AddIn.

Image: Reddoxx Logon Button

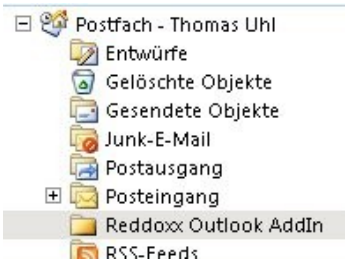
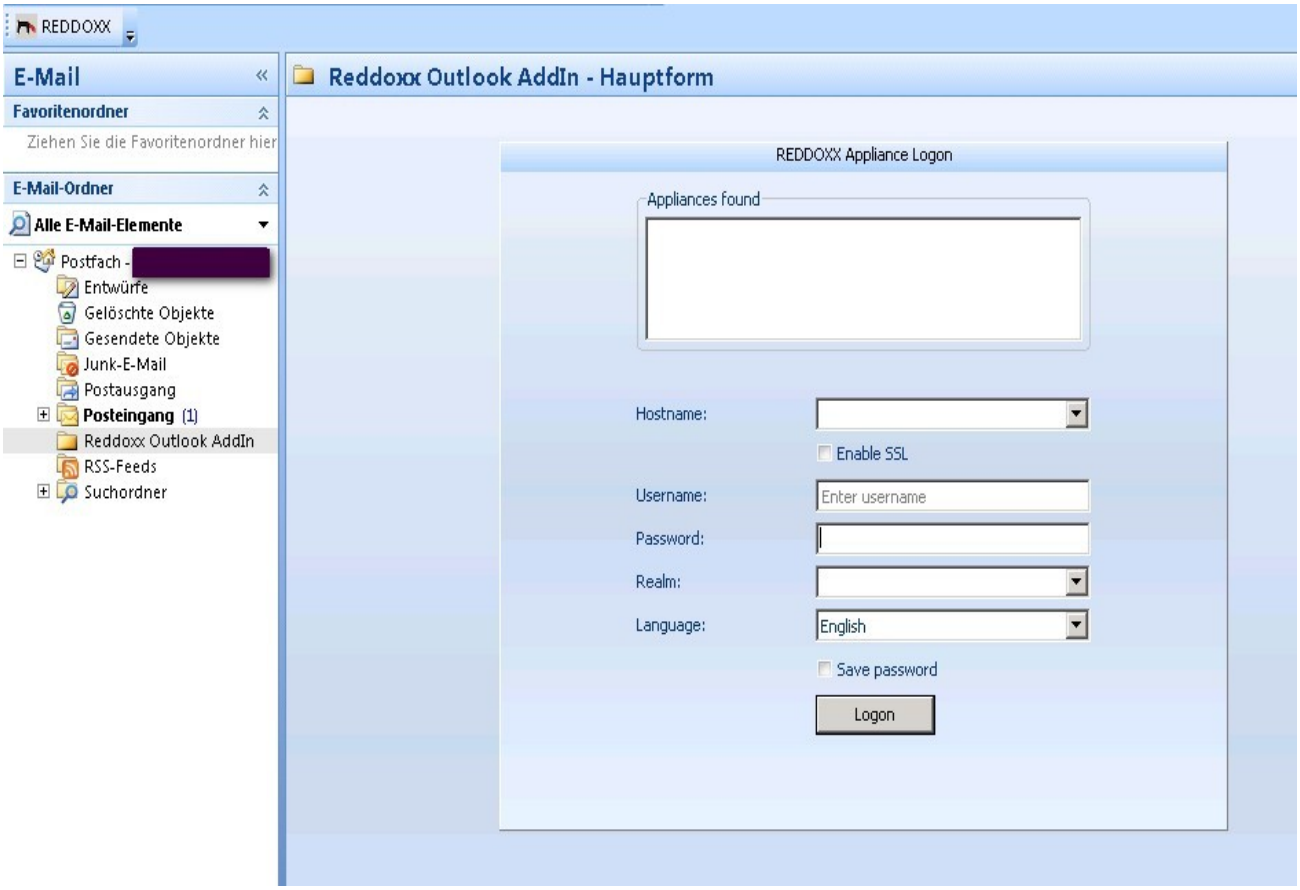


Image: Reddoxx Folder

With a click on the REDDOXX button or a click on the Reddoxx folder, the login screen appears.

4.3 REDDOXX Logon



NOTICE

The logon process is the same as to the User console logon detailed in Chap. 2.

4.4 The REDDOXX Menu

The design of the menu is similar to the user console. The difference is the menu items are shown horizontally on the bottom of the screen, instead of vertically on the left.

NOTICE

The menu items are the same as the user console menu items detailed in Chap. 3.

4.5 Message Archiving

You can retroactively archive mails or a complete folder from your mailbox to the REDDOXX Appliance.

1. Login to the REDDOXX Appliance.
2. Select the mail(s) from your mailbox and folder you wish to archive.

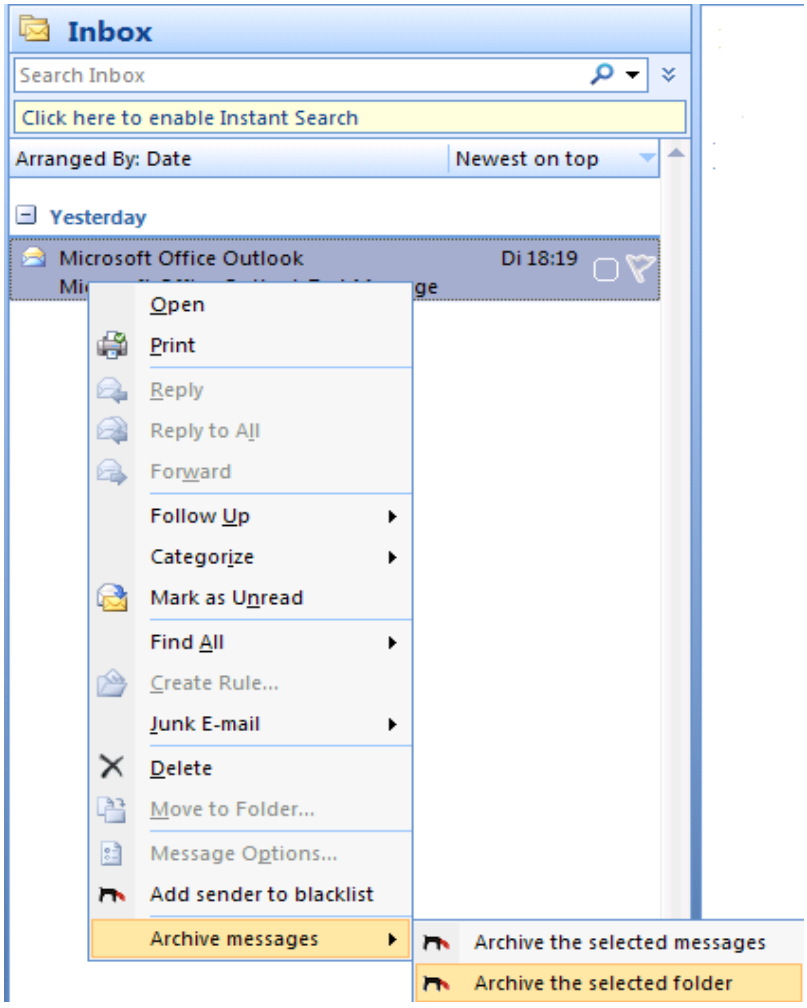


Image: Message archiving

3. Right click on the message you wish to archive. The context menu opens and shows the following options:
    - Archive the selected message
    - Archive the selected folder

NOTICE

If you choose “Archive folder“, each mail found in the selected folder will be listed in the archive window. Consider this if you are planning to archive thousands of messages because this can take quite an amount of time. All other options are the same as “Archive message”.

Before the archiving process starts, all selected e-mails are listed.

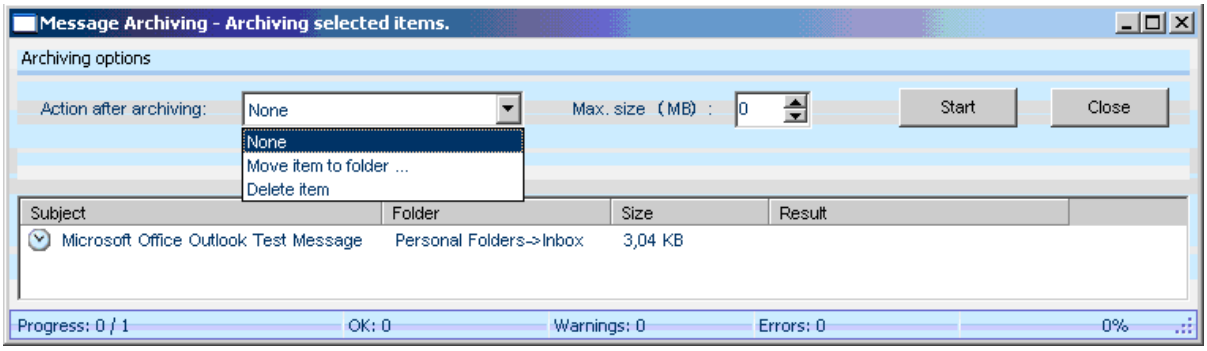


Image: Archive messages window

You can choose from the following options in the archiving window.

Action after archiving:

Move item to folder: After archiving has finished, the folder is moved to the specified folder.

Delete item: The message will be deleted when the archiving has finished.

None: No action is taken after archiving.

Max. size (MB): The size limit in mega bytes of a single message until it is archived.

Start: Starts the archiving process.

Close: Closes the archiving window.

During the archiving, the user can view the progress bar.

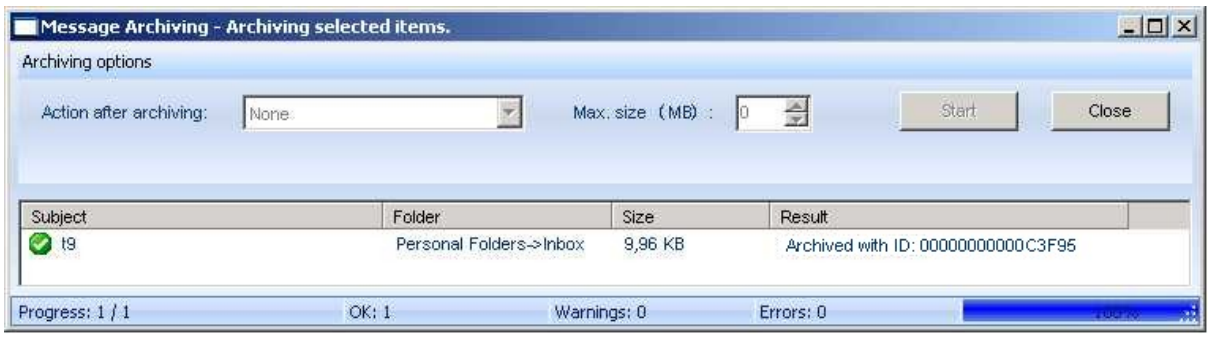


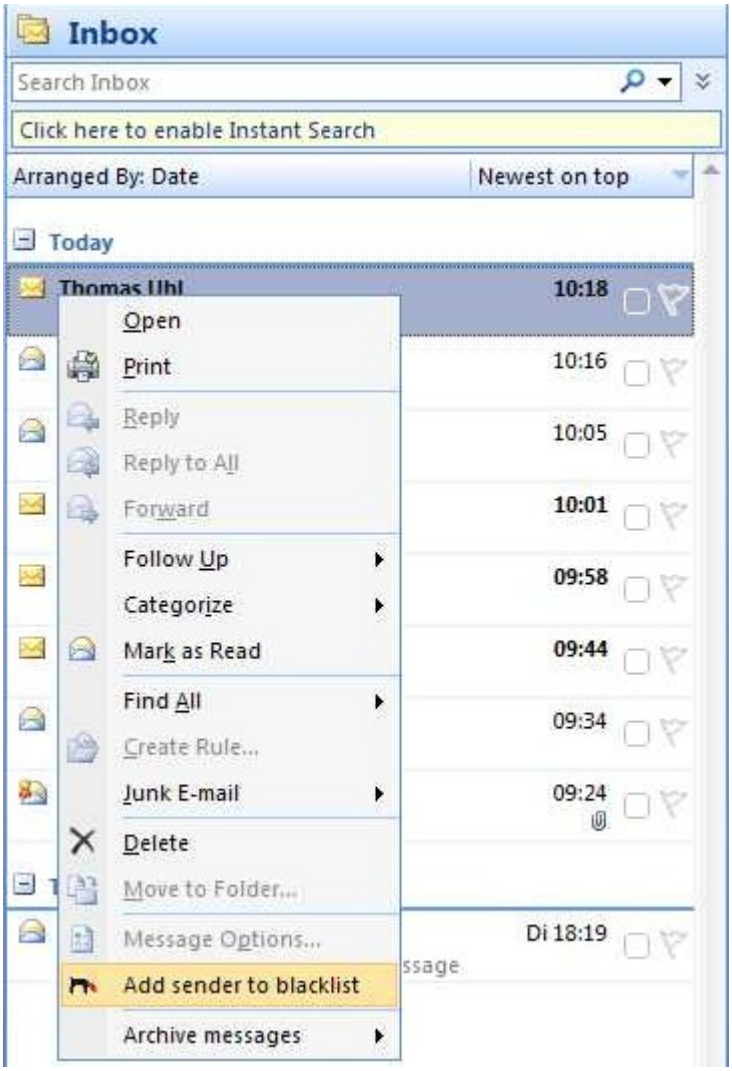
Image: Archiving messages dialogue with progress bar

4.6 Blacklist an e-mail manually

If an e-mail was not filtered by the appliance, you can manually set the sender address on the appliance's blacklist.

1. Select the e-mail and right click.

   The context menu opens.



2. Click on "Add sender to blacklist".

   The sender of the selected e-mail is shown in a new window for confirmation.

3. Blacklist domains:

   You also can block the complete domain if this option is enabled by the appliance policies. Contact your administrator if you need to have this feature enabled.

4. Click on „Add“.

   The sender is now added to the blacklist. The window closes.

5 Glossary

A

ABL Filter:

Address Blacklist Filter – checks the sender address against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The lists are maintained manually by the administrator or the user.

Advanced RBL Filter:

Advanced Realtime Blacklist Filter - All email servers involved in the transport of the incoming mail are checked against public blacklist servers. We do not assume any guarantee for the function of the selected blacklist servers as well as the absence of errors in the listed entries on the blacklist servers.

Appliance:

The REDDOXX appliance is the basic component of the REDDOXX program. There are several variants of the REDDOXX Appliance and there are both hardware and virtual appliances available. This ensures that the demands of all sizes of companies and e-mail traffic are optimally covered. Observe the warning and safety notices!

AWL Filter:

Address Whitelist Filter – checks the sender address against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. Some filters update this list automatically. The lists can also be administered manually by the administrator or the user.

B

Bayes Filter:

Via a content check, the Bayes filter determines the spam probability. Spamfinder automatically defines the word lists. We do not assume any liability for false detection.

C

CISS:

Confirmation Interactive Site Server, in short CISS, is a unique, multiple stage control process, which ensures the permanent exchange of wanted mails between sender and receiver. Intelligent authorization of the sender by means of CISS (registered for patent), a unique challenge/response-functionality.

CISS Filter:

Confirmation Interactive Site Filter – This filter ensures that the sender is a human sender. For this purpose, a corresponding Internet page is provided via the Spamfinder portal, which is accessible in the Internet. The availability of the Spamfinder portal is at least 98.5% per year.

Cluster:

A cluster denotes a number of networked computers. These networked computers are available for parallel processing. Partial tasks belonging to a task are processed. Contrary to parallel computers, the load distribution takes place on the level of individual processes started on one or several machines in the cluster. Therefore you do not require parallel software or special operating systems, but instead a scheduler which assigns the partial tasks to the individual computers. Alternatively, clusters are also used to increase the availability of systems.

Console:

Software component with which the REDDOXX Appliance is controlled.

D

DBL Filter:

Domain Blacklist Filter – checks the sender domain against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The lists are maintained manually by the administrator or the user.

DMZ:

A DMZ means Demilitarized Zone. A DMZ is an intermediate network that is formed at network interfaces but does not belong to either of the networks. It represents an inherent network which is not as heavily secured as the network that is to be protected. With simple security gateways, a DMZ is usually generated at a third interface of the package filter. If the security gateway consists of an application level gateway-package filter, a different interface of the application level gateway (ALG) usually serves as the DMZ interface. If package filters or ALG have more than three interfaces, an additional DMZ can be formed.

DNS:

The Domain Name System (DNS) is one of the most important services in the Internet. The DNS is a distributed database that manages the name space in the Internet.

Domain:

A domain is a coherent section of the hierarchic DNS name space. Starting from its domain name, a domain always comprises the entire subordinate tree structure.

DWL Filter:

Domain Whitelist Filter – authorizes the sender domain against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The

lists are maintained manually by the administrator or the user.

F

Failover:

A failover denotes a technology in the IT sector which serves to keep data and services always readily available.

H

Host name:

The host name of the REDDOXX Appliance in the network.

L

LDAP:

LDAP (Lightweight Directory Access Protocol) is a network protocol applied for so-called directories. It handles the communication between the LDAP client (e.g. with a mail server or a digital address book) and the directory server. It offers all log-specific functions required for such communication: registration on the server, the search query and data modification.

M

Mail Hop:

A mail hop is when an email is transferred from one server to another. Each of these servers is considered to be a mail hop.

N

NBL Filter:

Network Blacklist Filter - checks the IP address of the email server against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The lists are maintained manually by the administrator or the user.

NWL Filter:

Network Whitelist Filter - checks the IP address of the email server against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The lists are maintained manually by the administrator or the user.

O

OS:

Operating System.

Q

Quarantine:

For all authorized users, the REDDOXX Appliance contains quarantine mailboxes, which can be configured individually. Together with the achieved false positive rates, this feature enables you to reach conformity with the valid laws.

R

RAID:

A RAID system (Redundant Array of Inexpensive Disks, aka Redundant Array of Independent Disks) serves to organize several physical hard disks of a computer to form a powerful and safe logical drive.

RBL Filter:

Realtime Blacklist Filter - The sending email servers are checked against public blacklist servers. We do not assume any guarantee for the function of the selected blacklist servers as well as the absence of errors in the listed entries on the blacklist servers.

Realm:

A realm is similar to a domain in which the user authenticates him/herself. (Also see the chapter: "User Administration - Login Configuration")

RVC Filter:

Recipient Verify Check Filter - To protect the local email server from "spam floods", the recipient address is checked by asking the respective email server, whether the recipient is known. This function is currently available for Microsoft Exchange Server as of version 5.5.

S

SBL Filter:

Subject Blacklist Filter – Checks the email subject against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The lists are maintained manually by the administrator or the user.

SMTP:

Simple Mail Transfer Protocol. This protocol formats an email with more information than just sending the mail "as is". The protocol has several functions. On the one hand, SMTP lets your emails go straight to the receiver, on the other hand, SMTP enables routing your emails via different servers, so-called MTA (Mail Transfer Agents), to the recipient. Almost all email clients use this protocol to send electronic mail.

SRC Filter:

Sender Receive Check Filter - Checks whether the sender accepts an incoming mail. False spam detection, e.g. with newsletters or other automatically generated emails, cannot be completely ruled out, but can be prevented by making the respective entries in the positive filter lists.

SWL Filter:

Subject Whitelist Filter – Checks the email subject against a list maintained in the Spamfinder. The entries can be made both individual user-related, as well as company-wide. The lists are maintained manually by the administrator or the user.

T

TCP/IP:

Transmission Control Protocol / Internet Protocol. TCP/IP is the protocol that controls the connections/data exchange between computers in the Internet. When transmitting information, TCP divides the sent data into small packages, gives them a check sum (transmission safety) and numbers them consecutively (to ensure that the packages are reassembled again in the correct sequence). The TCP packages also contain the addresses of sender and receiver (IP addresses).

V

Virus Scanner:

The virus scanner checks the attachments of all emails for viruses. Packed files are temporarily unpacked and checked. Emails in which a virus is detected are saved in the quarantine section. Only the administrator has access to quarantine section. The Spamfinder obtains the virus signatures directly from the scanner manufacturer (ClamAV). REDDOXX does not assume any guarantee for the topicality of the signature files, as well as the availability of the signature server. REDDOXX does not assume any liability for damage caused by undetected viruses.